WEATHERING THE CYBER STORM: THE MILITARY'S RESILIENCY TO CYBER ATTACKS IN FUTURE WARFARE

BY

STEVEN T. WIELAND, MAJ, USAF

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2012

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

COLONEL SUZANNE BUONO

COLONEL MELVIN DEAILE

DISCLAIMER

ABOUT THE AUTHOR

Major Steven Wieland was a 1999 graduate of the United States Air Force Academy, where he majored in computer science. Subsequent to graduation, he was commissioned as a communication officer. Additionally, Major Wieland received master's degrees in business administration and military operational art and science from the University of Maryland, University College and the Air University, respectively. He has a held a variety of assignments in communications and cyber operations, culminating in his last post as the Chief Communications Officer, White House Situation Room.

ACKNOWLEDGMENTS

I want to thank the faculty at SAASS. Nearly all of them had a hand in some part of process. My advisor, Col Suzanne Buono, provided encouragement and guidance throughout the process. Nearly half of the faculty graciously offered their time to answer questions on a variety of topics related to this thesis. I truly appreciate their assistance. I would be remiss if I did not mention my course instructors, many of whom unwittingly received a section of my thesis as part of the course paper. Their feedback was invaluable.

I especially want to thank my wife, who was a constant source of encouragement throughout the entire year. Her exceptional writing skills, though intimidating at times, were the best resource for an average writer. Yet, her constant love was the best resource for any man, as it encouraged me to continue when I wanted to give up. I thank you and love you with all my heart.

ABSTRACT

This study examines what the military should do to be resilient against cyber attacks. Its basis rests on two major assumptions. First, it assumes the United States' adversaries will attempt to use attacks against the military. Second, it assumes some of these attacks will be successful despite established defenses. The military must be prepared to continue its mission despite cyber attacks.

To do so, the military must act along two major axes of effort. First, those units that use cyberspace—combat units and support units—must develop procedures to operate in a denied or degraded cyber environment. This process requires them to assess areas that have become reliant on cyberspace. A robust analysis forces the units to consider everything from the technology they use to the way they train their leaders. The units then must exercise the procedures developed from this analysis and adequately train personnel. Second, those responsible for cyber defense must ensure the effects of a cyber attack are fleeting. Alternate operating procedures utilize military force sub-optimally. Cyber defenders use a mix of active and passive defenses to halt the attack. Their goal is to restore service and allow military units to return to normal operating procedures, and thus, restore military capability. Cyber defenders must integrate with the more traditional forms of operations. They must have the wherewithal to posture themselves and react in a manner most conducive to the operating force. The organizational structure must change to accommodate this integration.

CONTENTS

Illustrations

CHAPTER 1

INTRODUCTION

The US government's digital infrastructure now gives the United States critical advantages over any adversary, but its reliance on computer networks also potentially enables adversaries…to impede the United States' conventional military forces.
William J. Lynn III, Deputy Secretary of Defense

The conventional wisdom is the United States is more dependent on information technology than any other nation.[1] The former Director of National Intelligence stated in Senate testimony, "We're the most vulnerable, we're the most connected, and we have the most to lose."[2] Though steps can be taken to mitigate vulnerabilities, the risk cannot be eliminated completely. Deputy Secretary of Defense William Lynn advocates for resiliency and a more agile concept of operating in cyberspace, "In an offensive-minded environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun."[3]

The term "resiliency" is bantered around in the National Security Strategy and other high-level strategic guidance throughout the Department of Defense.[4] The collective implications of these documents are that the military benefits tremendously from cyber technologies. The modern military, and indeed modern society, is not just dependent upon cyberspace, it is integrated into cyberspace. Furthermore, the strategic

---

[1] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 28.
[2] J. Nicholas Hoover, "Former Intelligence Chief: U.S. Would Lose Cyberwar," *Information Week*, 23 February 2010, http://www.informationweek.com/news/government/security/223100425 (accessed 23 January 2012).
[3] William J. Lynn, III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.
[4] See The White House, *National Security Strategy*, May 2010; The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011; Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership*, 8 February 2011; Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011. Resilience is a dominant theme throughout the 2010 *National Security Strategy*, including specific references to cyber resilience (pg. 27). "Enhancing security, reliability, and resilience" is a major policy priority in the *International Strategy for Cyberspace* (pg. 18). The other documents echo similar sentiments, including the 2010 *National Military Strategy*, which states, "Our ability to operate effectively in space and cyberspace, in particular, is increasingly essential to defeating aggression…We must grow capabilities that enable operations when a common domain is unusable or inaccessible" (pg. 9).

guidance suggests potential adversaries recognize the United States' strategic advantage and will engage in cyber warfare to deny it. The military must plan for the enemy to deny, disrupt, or corrupt cyber assets.

The fact cyber warfare is still in its infancy complicates the discussion on how to be resilient against an attack. To date, the overwhelming majority of practical experience with hostile cyber actions comes from criminals and intelligence collection. Cyber warfare resembles the position of pre-World War I airpower. Prior to World War I, airpower was used for reconnaissance and limited, militarily inconsequential attacks.[5] Yet, all of the Western powers saw potential in airpower—at least enough potential to acquire aircraft. Similarly, militaries see potential in the use of cyber power, but as was shown with airpower, the use of a nascent weapon of war may evolve in unpredictable and evolutionary ways.[6] The unknown character of cyber warfare makes detailed planning impossible. Militaries preparing to withstand a cyber attack have very little historical context, and the historical context may not be particularly relevant.

This uncertainty is not an excuse to absolve the military's need to strive for resiliency. The United States military has not had to operate in an environment where the enemy was using chemical weapons for nearly 100 years. However, the military still prepares for the possibility, even though the context in which chemical weapons would be used is dramatically different. It has developed equipment to deal with a chemical threat. It trains its people and conducts exercises to reinforce these skills.[7] Particularly for fixed locations, such as airbases, the ability to operate immediately after an attack, even if in a somewhat degraded state, and to recover fully in the shortest possible time is a major concern. Likewise, resiliency from cyber warfare dictates the military continue to operate in the face of enemy cyber attacks and to restore full capability in a short period time. To date, the military has not training aggressively to do so.

---

[5] Lee Kennett, *The Air War: 1914-1918* (New York: Free Press, 1999), 17-20. Prior to World War I, airplanes had been employed in conflicts in North Africa, the Balkans, and Mexico. Military aviation began with reconnaissance and pilots dropping weapons on their own initiative from the aircraft.

[6] While the analogy between the advent of air warfare and cyber warfare has parallels, it is important not to take this analogy too far. At the beginning of World War I, neither the militaries nor civilian society were dependent upon the aircraft for much of anything. The aircraft was essentially a military experiment. Cyberspace, on the other hand, has become an important aspect of both military operations and civil society.

[7] See Kevin R. Beeker, "Strategic Deterrence in Cyberspace" (Master's thesis, Air Force Institute of Technology, June 2009), 41.

The field of critical infrastructure protection faces some of the same challenges as ensuring cyberspace's availability for military use. Critical infrastructures (water, power, transportation, etc.) tend to be complex systems.[8] They have a high degree of interconnectivity with other systems. An aberration in one part of the system may generate effects that are difficult to foresee across another system. An example of this is the DOD's reaction to the Code Red worm in 2001. In an effort to mitigate the effects of the worm, the DOD cut off web traffic between the NIPRNET—the DOD's unclassified network—and the Internet. One of the unintended side effects was that the Army Corps of Engineers was unable to control the locks on the Mississippi River, which were controlled via signals sent across the NIPRNET.[9] Those defending the NIPRNET backbone could not have reasonably foreseen the impact on the nation's transportation infrastructure.

Since critical infrastructures are complex systems, using linear processes with a step-by-step approach for planning, preparedness, response, and recovery is incompatible with the problem at hand. The best way to reduce risk is to focus on adaptability (i.e., resilience) rather than pure protection. A protective approach focuses on assets, hardening security, and the costs involved. It deals in absolutes—either something is secure or it is not. Resilience, on the other hand, focuses on the services a system provides, redesigning processes, and the benefits obtained from the system. In lieu of absolutes, a resilient approach accepts a sliding scale between secure and insecure.[10] In an environment of known threats, known adversaries, known capabilities, and with predictable outcomes, a protective strategy may be appropriate. In an uncertain world, resiliency may be a better approach. However, the real world requires a balance between the static order of protection and the adaptability of resilience. This balance is akin the being on complexity theory's edge of chaos.[11]

---

[8] Telecommunications and information technology are considered critical infrastructures as well.
[9] Andy Ogielski, "Securing the Global Network Infrastructure," white paper, (Renesys Corporation, 2005), http://www.renesys.com/tech/notes/WP_SGNI_rev2.pdf (accessed 18 January 2012).
[10] Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm," in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience* (Arlington, VA: George Mason School of Law, February 2007), 13-15.
[11] Louise K. Comfort, "Risk and Resilience: Interagency Learning Following the Northridge Earthquake of 17 January 1994," *Journal of Contingencies and Crisis Management* 2, no. 3 (September 1994): 159.

The meaning of resilience is in the eye of the beholder. No standard definition of resilience exists. John McCarthy of the George Mason School of Law chooses to describe resiliency using a boxing analogy, "Protective measures—a boxer's glove work, footwork, tucking, and ducking—and robustness—his endurance, reach, and stamina or ability to 'go the distance'—account for much of his skill sets, but resilience is an equally crucial element. Here, the idea of resilience is two-fold: 1) recovering from an immediate punch and continue the fight in the short-term, and 2) losing a fight, but having the ability to recover and continue fighting in the long-term."[12] As McCarthy points out, resilience has both long-term and short-term components. In essence, it is the ability to provide a degree of order out of chaos.

The response following the 1994 earthquake in Northridge, California provides a good illustration of a combination of protective and resilient measures. From a protective standpoint, the responders knew the earthquake threat well. Officials could take measures to defend against an earthquake's harmful effects, including research, legislation, and prescriptive training. Previous earthquakes provided a historical basis and tested the system. Other types of incidents—riots, floods, fires, etc.—augmented the responders' knowledge. Moving toward a more resilient standpoint, earthquake science is relatively new and uses relatively untested technologies. The lack of knowledge on how the technologies will react in a particular type of earthquake and in specific circumstances lends itself to chaos. After the Northridge quake, the responders found a situation that was very different than what was expected. In short, the response evolved over the course of the recovery. The responders' planning, preparedness, interactive communications, shared commitment, and chance allowed them to adapt in the face of chaos.[13]

This paper assumes and will provide anecdotal evidence that military cyberspace is also a complex system. As such, an aberration in cyberspace may produce effects both within and outside of the cyber domain. It also assumes America's adversaries will try to produce such an aberration to affect traditional military operations and that some of the cyber attacks will be successful. A degree of resiliency is required of traditional military units and of those charged with defending the cyber domain. This resiliency must be

[12] John A. McCarthy, "From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum," in *Critical Thinking*, 1-2.
[13] Comfort, "Risk and Resilience," 161.

checked with an appropriate level of protection. Of course, protective and resilient measures come at a cost, which must be balanced. The primary purpose of this paper is to analyze where this balance is and how much resiliency is appropriate.

Scope and Methodology

Several terms and concepts must be defined in order to frame this discussion. The first is cyberspace. The exact definition of cyberspace has varied throughout the years. It points to the difficulty civilian and military leaders have had in determining how to handle the new domain. In 2008, former Deputy Secretary of Defense Gordon England defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded controllers."[14] Yet, this definition is not altogether clear. What constitutes an "information technology infrastructure"? England's definition of cyberspace states "the" interdependent network, implying there is only one large network. What about a system that is theoretically a standalone computer to program the flight information into an aircraft? Is this computer part of cyberspace? Does it become part of cyberspace when updates are made to the computer via a flash drive or CD-ROM with information that came from a system that is recognized as part of cyberspace? Or for that matter, are aspects of the aircraft part of cyberspace? The ambiguity highlights the problem of deductively determining the bounds of cyberspace. Rather, one must work form the bottom-up to determine if a system is part of cyberspace.

The most obvious inclusions in cyberspace are Internet Protocol (IP) networks, such as NIPRNET, SIPRNET, or JWICS.[15] Many tactical data networks interact with at least one of the IP networks. For example, Blue Force Tracking (BFT) information can be viewed over the SIPRNET.[16] Additionally, applications such as databases, web servers,

[14] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 28.
[15] Internet protocol (IP) is the primary standard for communicating on the Internet. NIPRNET and SIPRNET are the military's unclassified and secret networks, respectively. The Joint Worldwide Intelligence Communications Network is a network for intelligence information across the US government.
[16] Rita Boland, "When Capabilities and Support Mean Life or Death," *SIGNAL Magazine*, March 2011, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2550&zoneid=285 (accessed 18 January 2012).

and messaging platforms (e.g., e-mail or chat) provide the relevant information to the user. Few would argue any of these systems are not part of cyberspace.

The telecommunications infrastructure is explicitly mentioned as a component of cyberspace in the DOD's definition of cyberspace. The telecommunications system uses many different media as links between nodes. Cell phones (including smart phones) use radios for at least the last leg of communications. Other links may include wired, terrestrial wireless, or space-based links. Paralleling the logic that includes web services and databases as part of cyberspace, one should also include applications that are transmitted across the telecommunications system as part of cyberspace by virtue of its dependence and interconnectivity. For instance, if a radar signal uses phone lines to connect an outlying radar antenna to its controllers, then that system is a cyber system. If the telecommunications system upon which it was dependent was inoperative either due to malfunction or due to attack, the radar signal would lose its utility unless resiliency was built into the system. Following this logic, industrial control systems and supervisory control and data acquisition (SCADA) systems, that is, systems that monitor and control processes in the physical world, are also a part of cyberspace. While predominately civilian in nature, SCADA systems are not exclusive to the private sector. Systems that use telecommunications lines to monitor base fuel tanks serve as an example of a military use of SCADA. Given the computerization and external communications of many modern aircraft, some aircraft systems are essentially SCADA systems that may have some degree of dependence on and vulnerability to cyber systems.

However, the most important part of cyberspace may be how the human interacts with it. Certainly, a human being is not a cyber asset, but if one accepts the DOD's official definition of an "information system," which is "*the entire infrastructure, organization, personnel, and components* for the collection, processing, storage, transmission, display, dissemination, and disposition of information,"[17] the human is critical to the information process. Cyberspace consists of diverse interconnected systems transmitted over multiple media; however, cyberspace ultimately serves humans beings. Although new computer chips can process information faster or hold more memory, the

[17] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 161 [Emphasis added].

human's processing capacity is relatively static. Furthermore, the human must ultimately decide whether to trust the data he is receiving or not. One must understand the human interaction to truly understand cyberspace and the impact it can have on military operations.

It is also important to define a cyber attack, or in other words, what constitutes an attack on cyberspace or its human interface. The DOD prefers to term computer network attack, which it defines as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[18] This definition suffers in two ways. First, it lacks specificity on what constitutes a computer network and how a computer network differs from cyberspace. Second, it ignores the possibility of the enemy altering data or otherwise engaging in deception. Thus, this paper uses the term cyber attack, defined as "actions taken through cyberspace to alter, deceive, or disrupt information in cyberspace or to destroy information or physical assets."[19] Cyber attack does not include kinetic strikes that originate outside cyberspace against cyberspace assets, nor does it involve the gathering of information for intelligence purposes. Unlike espionage, cyber attacks must do more than passive observation. While the ability to collect intelligence is important, it falls under a different rubric than warfare itself.[20]

Another term worth defining is mission assurance. The concept of mission assurance is not clearly defined within the context of cyberspace. The official DOD definition comes from the context of critical infrastructure protection. It defines mission assurance as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are

[18] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 67.
[19] Definition was inspired in part from William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics regarding U.S. Acquisition of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 1-2.
[20] See Jeffrey H. Smith, "Symposium: State Intelligence Gathering and International Law," *Michigan Journal of International Law* 28 (Spring 2007): 544, for an excellent discussion on the concept of international law and espionage. International law's silence on espionage coupled with customary international practices legitimize the espionage. On the other hand, hostile cyber actions that destroy or modify information goes well beyond the definition and international legitimacy of espionage.

available to the Department of Defense to carry out the National Military Strategy."[21] While intended for a different context, the definition is suitable for operations using cyberspace. The goal is not to protect cyberspace for cyberspace's sake; rather, it is to ensure the military can continue to carry out its missions. The combination of resiliency and protective measures set the environment for mission assurance.

Cyberspace is a big place, and any discussion of it must include appropriately scoping the problem. To effectively analyze what the military must do to garner the proper degree of resiliency to achieve mission assurance, this paper must limit the discussion regarding certain aspects of cyberspace and cyber warfare. First, this paper will only consider what is necessary to perform a military mission in the face of cyber attacks and not what is necessary to defend the homeland and civilian assets against cyber attacks. This exclusion does not neglect the importance of the civil use of cyberspace. Rather, it is an acknowledgement that outside of military-owned assets, the military plays a relatively minor role in defending the cyber domain.

An additional aspect of cyber warfare that has to be specifically included in any discussion of cyber resilience is the application of cyber warfare in the larger political context. Carl von Clausewitz's famous dictum—"war is merely the continuation of policy by other means"—also applies in cyberspace.[22] War in or through cyberspace cannot be separated from war itself any more than war and military force can be separated from politics. The military operates to achieve political objectives, a concept that must remain a central proposition throughout this analysis.

Chapter 2 starts this analysis by examining the benefits the military derives from cyberspace. The military cannot hope to achieve cyber resilience at an appropriate cost without understanding what benefits the harnessing of cyberspace brings. Chapter 3

---

[21] Department of Defense Directive (DODD) 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure*, 14 January 2010, incorporating Change 1, 1 July 2010, 19. The full definition is "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations."

[22] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87.

discusses the principles of cyber warfare and, more importantly, the characteristics that distinguish it from other domains of warfare. Chapter 4 follows the assumption that some cyber attacks cannot be stopped and looks at how traditional military units can continue to execute their assigned missions during a cyber attack. Chapter 5 follows with the actions cyber defenders must take to mitigate the harmful effects of cyber attacks and to restore the use of military cyberspace. Finally, chapter 6 pulls together themes from the previous chapters to draw conclusions on what the military must do to continue to operate in the face of cyber warfare.

CHAPTER 2

MILITARY BENEFITS OF CYBERSPACE

Traditionally, the military determines the amount of risk it undertakes by weighing the operational benefit, the vulnerability, and the threat. From there, the military either accepts risk or takes steps to mitigate it. This chapter focuses on the first step—determining the operational benefit of cyberspace. Since no equation exists to calculate the value of cyberspace, this chapter will look at theoretical valuation, evidence from recent conflicts, and benefits unrelated to actual combat experience. It will also examine some of cyberspace's major limitations and will summarize the net benefit.

Valuation of Networks and Connections

Metcalf's Law is a common axiom to determine the value of commercial networks. Per Metcalfe's Law, a network's value increases by the square of the number of users on the network.[1] Though commonly mentioned, Metcalfe's Law is not universally accepted nor is it based on scientific or mathematical laws. Others contend the growth in value of the network is actually closer to n log (n), where n is the number of users in the network. The slower growth rate is based on the assumption that each connection in the network does not necessarily have the same value.[2] Regardless of the valuation from the growth of the connections, Metcalf's Law and its derivatives attribute value to the number of connections and, thereby, the number of people and data sources an individual can reach.

The number of connections in a network does not tell the entire story. Clearly, a broadband network is more valuable than a dial-up network. Simple economics levy proof of this statement when consumers pay more for a broadband connection even though it offers them no more connections than with dial-up, just at a faster speed. Moreover, having more information is not necessarily better. Having the right information at the right time is often more important. A network that does not provide useful information has no value. Determining a network's value, therefore, depends on

---

[1] Stuart H. Starr, "Towards and Evolving Theory of Cyberspace," *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Fairfax, VA: IOS Press, 2009), 32.
[2] Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law is Wrong," *IEEE Spectrum*, July 2006, http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong.

many factors—the number of people in the network, the speed of the network, the availability of useful information, and the ability to present useful information in an understandable format—just to name a few. The solution to finding true value cannot be plugged into a formula. Value depends on a multitude of objectives and contextual factors.

Network-Centric Warfare Principles

The theory of network-centric warfare helps to explain some of the contextual factors applicable to the military.[3] Its general concept is to leverage the advantages of the information age to yield greater military power.[4] The desired outcomes of network-centric warfare include:

- better synchronization of events and consequences on the battlefield;
- the ability to make better decisions, faster;
- increased lethality, survivability, and responsiveness, especially through the use of precision.[5]

The four tenets of network-centric warfare support these desired outcomes and help to describe the power cyberspace brings to the military:

- a robustly networked force improves information sharing;
- information sharing enhances the quality of information and shared situational awareness;
- shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command;
- these, in turn, dramatically increase mission effectiveness.[6]

The final tenet is, of course, the ultimate goal. Network-centric warfare assumes military forces can operate more effectively if enabled by cyberspace.

It is important to note that the network-centric warfare concept is not an exclusively American idea. US allies have also adopted network-centric warfare ideas.

[3] This paper treats the concepts of network-centric warfare and network-centric operations—which includes military operations short of war—as synonymous. For consistency, the term "network-centric warfare" will be used.
[4] John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage," *Signal*, May 2003, 58.
[5] Department of Defense, *The Implementation of Network-Centric Warfare* (Washington DC: Office of Force Transformation, n.d.), 6.
[6] Department of Defense, *The Implementation of Network-Centric Warfare*, 7.

Australia, for example, sees a network-centric approach both as a way to integrate with the United States and as a way for its small force to "punch well above its weight."[7] The Australian approach recognizes two dimensions of network-centric warfare—the human dimension and the network dimension. The human dimension is predicated on professional mastery and the use of mission command, or the "the conduct of military operations through decentralized execution based on mission-type orders."[8] It assumes commanders will apply the information available to them to fulfill the superior commander's intent. The second dimension—the network dimension—consists of networked sensors and communications links. The network dimension links all military systems and commands and has a profound influence on the human dimension.[9]

The Australian perspective illustrates the coupling between the people charged with accomplishing the mission and the systems that enable them to do so. It also illustrates the role command and control (C2) plays. The United States' military has four C2 objectives in network-centric warfare. First, units should self-synchronize. In other words, unit commanders should take the initiative to act based the information on hand, rather than waiting for traditional orders from the headquarters. The second objective is an improved understanding of the commander's intent. Through more robust communications, unit commanders should better understand what their commander intends to accomplish. Third, the military will have better situational awareness at all levels of command. Fourth, the use of collaborative tools will help reduce the uncertainty of war.[10]

Zealots claim network-centric warfare transforms a force to near invincibility. Critics attack this view from several angles. Michael Schrage of the Massachusetts Institute of Technology's (MIT) Sloan School's Center for Electronic Business and a senior advisor to MIT's Security Studies Program cautions that lessons from business prove that more information—even better information—does not necessarily lead to

---

[7] Gary Waters, "The Australian Defence Force and Network-centric Warfare," in *Australia and Cyber Warfare*, eds. Gary Waters, Desmond Ball, and Ian Dudgen (Canberra: ANU E Press, 2008), 6.
[8] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 215.
[9] Waters, "The Australian Defence Force and Network-centric Warfare," 11.
[10] U.S. Library of Congress, Congressional Research Service, *Network-centric Operations: Background and Oversight Issues for Congress*, by Clay Wilson, CRS Report RL32411 (Washington, DC: Office of Congressional Information and Publishing, 15 March 2007), 3.

better decisions.[11] Specifically, he cites, "Fund managers 'knew' that there were speculative bubbles in the internet, telecom, and bio tech sectors. They invested anyway. Having the 'right' information at the 'right' time may not lead to the 'right' decision."[12] Aside from the possibility of commanders failing to make the right decisions, Alfred Kaufman argues network-centric warfare ignores the human component of information. Humans will have different perspectives on the same information. Just because information is shared does not mean that all parties share in their interpretation and understanding of it. He further argues that humans have difficulty dealing with conflicting information, a problem for which network-centric warfare fails to account.[13] Other criticisms include the potential for information overload, an overdependence on the information systems, and a lack of interoperability with allies.[14]

Network-centric warfare's critics temper the notion that it will produce or operate with perfect information. Yet, just because the network-centric warfare concept cannot produce perfect information does not mean that it loses its utility as a benchmark to measure value. It sets a point from which to measure and a goal for which to strive. The conflicts over the past several years provide evidence to the degree the network-centric warfare concepts have come to fruition.

The Use of Cyberspace in Operations Enduring Freedom and Iraqi Freedom

The military has used cyber technologies for a variety of applications since the advent of the modern computer. In many ways the integration of cyber technologies has been evolutionary. However, military operations since the 11 September 2001 terrorist attacks have leveraged cyberspace to such a large degree that many, if not most, military functions rely heavily on cyberspace.

[11] Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," Security Studies Working Paper E38-600 (Cambridge, MA: Massachusetts Institute of Technology, May 2003).
[12] Schrage, "Perfect Information and Perverse Incentives," 5.
[13] Alfred Kaufman, "Caught in the Network: How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy," *Armed Forces Journal*, 1 February 2005, 20-22.
[14] Waters, "The Australian Defence Force and Network-centric Warfare," 14-15. U.S. Library of Congress, *Network-centric Operations,* 23. John B. Tisserand, III, *Network-centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume III: Network-centric Warfare Insights* (Carlisle Barracks, PA: Center for Strategic Leadership, 2006), 20-21.

Operations Enduring Freedom and Iraqi Freedom serve as cases to determine the value of cyberspace to the military. Nevertheless, it is important to avoid confusing the value cyberspace provided to these operations with the value the military provided. In many cases, one could point out where the military did not meet its political objectives. The goal of this section is not to evaluate the utility of or the execution of military operations. Rather, it intends to analyze what value cyberspace added to military force in the course of achieving its desired political objections.

Operation Enduring Freedom

Operation Enduring Freedom was the military's portion of the United States' response to the 9/11 terrorist attacks. In a joint address to Congress, President George W. Bush laid out his objectives. First and foremost, "Our war on terror begins with al-Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated."[15] In the same speech he specifically set political goals for the upcoming mission in Afghanistan. He called upon the Taliban to turn over al-Qaeda leaders; release unjustly imprisoned foreign nationals; protect foreign aid workers, journalists, and diplomats; close all terrorist camps; and grant the US access to the camps. If the Taliban did not comply, the United States would consider it an enemy as well.[16]

After the Taliban failed to accede to the United States' demands, the president ordered military action in Afghanistan. The objectives, based on President Bush's speech, included overthrowing the Taliban government and dismantling al-Qaeda's ability to operate in Afghanistan. Further guidance from the Secretary of Defense included the goals of developing relationships with Taliban opponents, providing humanitarian relief operations, and minimizing collateral damage. The implicit objective was to send a clear message around the world—harboring terrorists who attack the United States will result in swift, decisive military defeat.

[15] George W. Bush, "Address Before a Joint Session of Congress on the United States Response to the Terrorist Attacks of September 11," Compilation of Presidential Documents, 37 WCPD 1347 (20 September 2001): 1358, http://www.gpo.gov/fdsys/pkg/WCPD-2001-09-24/pdf/WCPD-2001-09-24-Pg1347.pdf (accessed 28 April 2012).
[16] Bush, "Address Before a Joint Session of Congress on the United States Response to the Terrorist Attacks of September 11," 1348.

The first phase of Operation Enduring Freedom in Afghanistan used special operations forces (SOF) to liaise with anti-Taliban Afghan forces in order to topple the Taliban and to destroy al-Qaeda elements. The SOF forces relied heavily on airpower armed with precision weapons to provide firepower. Military historian Stephen Biddle described this "Afghan Model" of war as using unskilled local militias to "screen US commandos from the occasional hostile survivors and occupy the abandoned ground thereafter."[17] While the use of SOF backed by aircraft was an important aspect of the campaign, the fact that combat operations were even able to commence in an area where the United States' military had very little infrastructure or experience a mere three weeks after the attacks is also important. Within 60 days, a few hundred American ground forces had effectively removed the Taliban from power.[18]

The speed and power of the operation undoubtedly sent a message that the United States could strike anywhere in the world. In this case, it did not have to wait for the logistics machine to transport conventional military formations and supplies to the battlefield prior to conducting military operations. By January 2002, a mere 2,000 troops were on the ground in Afghanistan, a testament to highly distributed nature of combat in Afghanistan.[19]

It was the use of cyberspace that compensated for the lack of force on the ground, and it successfully facilitated the start of the campaign. To do this, planning had to be accelerated. The US Central Command (USCENTCOM) commander and the majority of his staff were able to remain in Tampa while communications and support teams established forward headquarters in Kuwait and Uzbekistan.[20] The communications teams provided the forward headquarters with connectivity and collaborative tools that kept all parties linked together. At the tactical level, SOF teams at the forward bases could ensure they had the latest maps and information on friendly and enemy forces prior to going into the field. Once in the field, the teams could communicate back to their headquarters and to coalition aircraft through a variety of radios and satellite phones. Due

---

[17] Stephen Biddle, "Afghanistan and the Future of Warfare," *Foreign Affairs* 82, no. 2 (March/April 2003), 31.
[18] Richard W. Stewart, *Operation Enduring Freedom: The United States Army in Afghanistan, October 2001-March 2002* (Washington, DC: Center for Military History, 2004), 27.
[19] Stewart, *Operation Enduring Freedom*, 29.
[20] Robert K. Ackerman, "Operation Enduring Freedom Redefines Warfare," *Signal*, September 2002, 3.

to the impracticality of carrying laptops into combat, deployed SOF operators usually only had a voice communications capability. Data capability was typically available at mid-level (i.e., those commanded by an O-5) headquarters and above.[21] While the headquarters was able to get a good common operating picture with known locations of friendly and enemy forces, this picture could not be passed down to the operators. That said, the ability for SOF headquarters to connect to conventional Air Force and Army data systems facilitated a tighter integration between the air platforms and combat service support units and, thereby, provided better air support and logistics.[22]

The use of cyberspace by conventional air units also had advantages. The incorporation of networked sensors (SOF, Predators, Global Hawk) into the air component command and control system allowed fighter, bomber, and armed unmanned aircraft to strike emerging targets. Data links allowed pilots to deconflict targets. Furthermore, the precision gained from laser and global positioning system (GPS) guidance transformed air support. Long-range bombers leveraged the ability to loiter to service multiple targets.[23] All of this made use of scarce assets operating from distant bases and lessened the likelihood of civilian casualties.

While Operation Enduring Freedom is typically associated with operations in Afghanistan, Operation Enduring Freedom encompasses operations in other geographic areas as well. In the Sahel and the Philippines, the military role mainly focuses on assisting and advising the local security forces. In both regions, cyberspace plays a surprisingly important role. United States Africa Command recognizes cyberspace's value so much that it lists exchange of military information and interoperability of communications systems as its first two goals of Operation Enduring Freedom-Trans Sahara.[24] In Operation Enduring Freedom-Philippines, a major emphasis is training the Philippine military to use information from US sources, to include the Predator

---

[21] O-5 headquarters include Special Forces battalions and SEAL teams. Robert K. Ackerman, "Special Operations Forces Become Network-Centric," *Signal*, March 2003, 17.
[22] Robert K. Ackerman, "Air Force Communicators Move Faster, Lighter," *Signal*, September 2002, 47.
[23] Ackerman, "Special Operations Forces Become Network-Centric," 17. Also Jeffrey L. Groh, "Network-centric Warfare: Leveraging the Power of Information," in *US Army War College Guide to National Security Issues, Vol. 1: Theory of War and Strategy*, 3rd ed. (Carlisle Barracks, PA: Army War College, 2008), 325.
[24] United States Africa Command, "Operation Enduring Freedom Trans Sahara," http://www.africom.mil/oef-ts.asp (accessed 21 February 2012).

unmanned aerial vehicle and the P-3 Orion maritime patrol aircraft. In each case, the military is taking steps to use cyberspace to help integrate allied forces. While the true value of this cyber integration will take years to unfold and may not be made public due to the relative low-visibility of the operations, it provides evidence of the value of sharing near real-time information with our allies in order to further mutual interests.

Operation Iraqi Freedom

The political objectives for Iraq included a combination of the overthrow of Saddam Hussein's government, the elimination of the threat posed by Iraq's presumed weapons of mass destruction, and the denial of sanctuary and support to terrorists within Iraq. The new regime was to be a stable, democratic, and territorially sound. Finally, as in Afghanistan, the United States would provide humanitarian assistance to Iraqi citizens.[25]

The military objectives required the defeat of Iraqi military formations loyal to Saddam Hussein. As with Afghanistan, the ferocity and the velocity of the campaign was a tool to communicate a stern message to other states. In response, US Air Forces Central declared a part of the desired end state as "[s]uccess in Iraq leveraged to convince or compel other countries to cease support to terrorists and to deny them access to [weapons of mass destruction]."[26] Any weapons of mass destruction capability had to be neutralized, and the government could not be allowed to remain in any fashion. In short, the overarching military objective was the complete destruction of the military apparatus that enabled Hussein to stay in power.

The force structure in Operation Iraqi Freedom was substantially larger than in Afghanistan. However, ground units still fought using relatively small combat units distributed across a large swath of territory to a degree never before experienced by a conventional force. With this construct, made possible through the use of cyberspace, the

---

[25] George W. Bush, "Address to the United Nations General Assembly in New York City," Compilation of Presidential Documents, 38 WCPD 1529 (11 September 2002): 1529-1533, http://www.gpo.gov/fdsys/pkg/WCPD-2002-09-16/pdf/WCPD-2002-09-16-Pg1529.pdf (accessed 28 April 2012); George W. Bush, "Address to the Nation on Iraq," Compilation of Presidential Documents, 39 WCPD 338 (17 March 2003): 338-341, http://www.gpo.gov/fdsys/pkg/WCPD-2003-03-24/pdf/WCPD-2003-03-24-Pg338-2.pdf (accessed 28 April 2012); *Authorization of the Use of Military Force Against Iraq of 2002*, Public Law 107-243, 107th Cong., 2nd sess., 16 October 2002; Report of CENTAF Assessment and Analysis Division, "Operation Iraqi Freedom – By the Numbers," 30 April 2003, http://www.globalsecurity.org/military/library/report/2003/uscentaf_oif_report_30apr2003.pdf (accessed 22 February 2012).

[26] Report of CENTAF Assessment and Analysis Division, "Operation Iraqi Freedom – By the Numbers," 30 April 2003, 4**.**

United States' military defeated a force of 350,000 soldiers while taking relatively few casualties.[27] The US Army Center for Strategic Leadership credited superior situational awareness for much of the success. Blue Force Tracking (BFT), for example, used GPS to show the precise location of units down to the company level, preventing fratricide and giving higher-level commanders a view of the battlefield never before attained in modern warfare.[28] The Force XXI Battle Command Brigade and Below (FBCB2) system provided units the ability to see a common operating picture, overlaid with maps and BFT data, and passed C2 messages down to the company level (see figure 1). This information was transmitted using commercial satellites and distributed horizontally and vertically across multiple echelons of command. Military satellites augmented FBCB2 to provide a greater degree of connectively and situational awareness.[29] The study concluded that improved situational awareness enhanced mission effectiveness. "[T]he introduction of extended reach communications and networked information systems significantly enhanced the ability of US Army commanders to make faster decisions, more easily exploit tactical decisions, more easily exploit tactical opportunities, conduct coordinated maneuver while advancing further and faster than at any previous time and more fully integrate and synchronize joint fires; all of which resulted in the rapid defeat of Iraqi military forces and the fall of the Ba'athist regime in Baghdad."[30]

[27] Dave Cammons et al., *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume I: Operations*, (Carlisle Barracks, PA: US Army War College, 2006), 19-20.
[28] Cammons et al., *Network Centric Warfare Case Study,* 25-54.
[29] John B. Tisserand, III, *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume III: Network-centric Warfare Insights*, (Carlisle Barracks, PA: US Army War College, 2006), D-2 – D-4.
[30] Kevin J. Cogen and Raymond G. DeLucio, *Network-centric Warfare Case Study: US V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Arp 2003)*, *Volume II*, *A View of Command, Control, Communications, and Computer Networks at the Dawn of Network-centric Warfare*, (Carlisle Barracks, PA: US Army War College, 2006), xi.

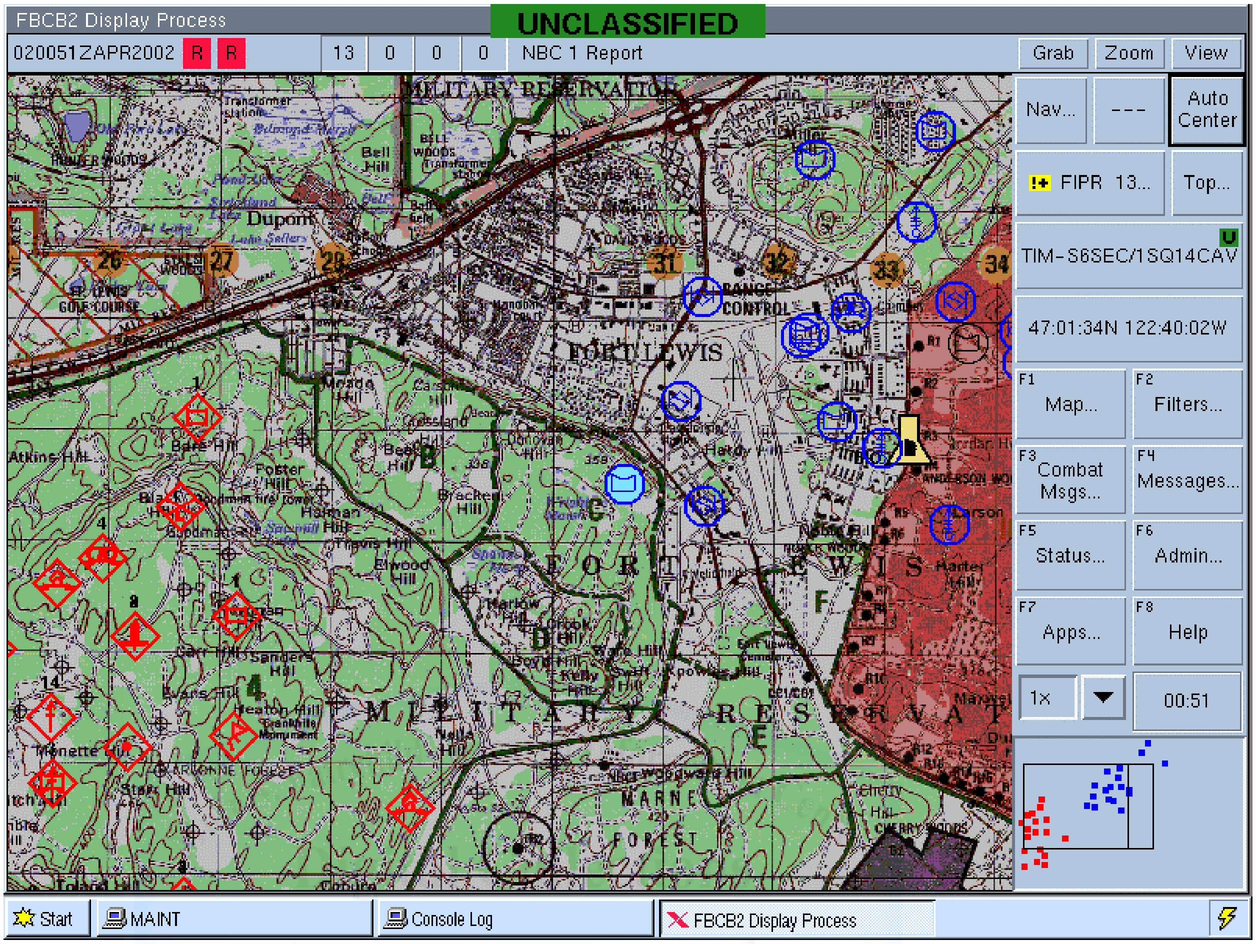

Figure 1: Sample FBCB2 Display

Source: Briefing, TRW/Raytheon, subject: FBCB2 Overview (Force XXI Battle Command – Brigade and Below), 30 April 2002

The logistical demands of Operation Iraqi Freedom differed substantially from those in Afghanistan. Resource-consuming armored and mechanized forces quickly moved through Iraq. Concurrently, the Army's concept of logistics changed from a stockpile system to a distribution system. The distribution system limited forward units to only enough supplies to cover small contingencies. It also allowed forces, however, to remain lighter and move faster, giving them the element of surprise. Furthermore, the close air support procedures evolved with the integration of Army and Air Force cyber systems. These systems, coupled with the use of GPS-guided Joint Direct Attack Munitions (JDAM) to service the Army's requests, meant that the Army did not have to

bring as much ammunition and supplies to the front, reducing the burden on an overwhelmed logistics system.[31]

The excess risk associated with such a distribution system was offset by the use of cyber systems that were able to predict which supplies would be needed for forward units and, with the use of in-transit visibility, to allow forward units to plan more effectively.[32] The speed of the campaign meant that some of the supply routes were not fully secured. The use of text messaging and two-way satellite communications allowed maneuver and logistics commands alike to have in-transit visibility on convoys. This allowed the headquarters to reroute convoys or warn them of possible enemy action in the area.[33] Although the logistics systems were not perfect, compared to manual reporting they cut off a day of latency and reduced uncertainty on the battlefield.[34]

The net result of the use of cyberspace in Operation Iraqi Freedom was that it allowed a relatively small force to take over a country twice the size of Idaho with unprecedented velocity. It enabled forces to move lighter and coordinate better. Cyberspace allowed the military to do things it otherwise could not have done.

Urban Warfare

Some may contend that the concept of network-centric warfare and cyber-enabled forces have limited value in an urban warfare environment, where the fighting is block-to-block and is intensely personal. Experiences in Iraq, however, suggest cyberspace does provide significant value in such scenarios. Overhead ISR assets, which distributed video to multiple units and levels on command, help to track the enemy. It denied sanctuary and caused the enemy to think that there was no escape. Furthermore, the precision gained by cyber technologies meant the military no longer had to destroy large portions of a city in order to root out insurgents.[35] A military force enabled by assets in cyberspace is more

---

[31] Cammons et al., *Network-centric Warfare Case Study*, 34.
[32] Eric Peltz et al., *Sustainment of Army Forces in Operation Iraqi Freedom: Battlefield Logistics and Effects on Operations* (Santa Monica, CA: RAND Corporation, 2005), xi-xii.
[33] John B. Tisserand, III, *Network-centric Warfare Case Study*, 92-93.
[34] Logistics units faced problems with incompatible systems, even between Army units. Furthermore, moving convoys and headquarters created communications dead spots. These difficulties contributed to a less than ideal logistical situation. However, on the whole, the systems facilitated a net gain in combat effectiveness. Eric Peltz et al., *Sustainment of Army Forces in Operation Iraqi Freedom*, 69-70.
[35] Rodney Pringle, "NCW Changing Urban Warfare, Official Says," *Aviation Week*, n.d., http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?headLine=NCW%20Changing%20Urban%20Warfare,%20Official%20Says%20%20&storyID=news/NCW02035.xml (accessed 21 February 2012).

effective in urban warfare due to its ability to obtain information and reduce civilian casualties.

Non-Empirical Contribution to National Security

The examples from Operations Enduring Freedom and Iraqi Freedom help show how military combat has been transformed by the benefits of cyberspace. However, the military value of cyberspace goes well beyond operations in Iraq and Afghanistan. Cyberspace changes combat power and allows the force being used in new ways. Among the many examples, cyberspace enables the effective use of a smaller and cheaper force, requires the deployment of fewer resources, facilitates the efforts of supporting commands, and takes advantage of common business practices.

Enhancing Combat Power and Reconfiguring the Force

The use of cyberspace enhances a force's combat power in ways not seen during recent conflicts. A 2006 RAND study compared the performance of F-15 sorties using Link-16 in simulated air-to-air combat compared to those with only a voice capability. The study concluded that not only did the F-15s using Link-16 "kill" approximately 2.5 times the number of enemy aircraft, the use of Link-16 yielded more flexibility, enabled faster decisions, and helped pilots choose more appropriate tactics.[36] Similarly, a study at the Joint Readiness Training Center showed that a Stryker Brigade Combat Team equipped with collaborative tools and modern voice and data networks collected better information on friendly and enemy forces, made dramatically faster decisions, and took 10 times fewer causalities than a legacy infantry brigade.[37] Furthermore, the digital systems gave soldiers the capability to retrieve mission data; whereas, soldiers previously had to rely on memorization or written notes.[38]

Additionally, the ability to command and control a fast moving, mobile force is made possible by cyberspace. By the late 19th century, the Prussians concluded a company was the largest unit capable of being commanded by a single person.[39] At that point in time, technology could not allow for anything more than couriers transmitting

---

[36] Daniel Gonzales et al., *Network-centric Operations Case Study: Air-to-Air Combat with and without Link-16* (Santa Monica, CA: RAND Corporation, 2005), xxix, 78. Link-16 is a tactical data link that shares radar tracks, friendly and enemy positions, and other information.
[37] David Gonzales et al., *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, CA: Rand Corporation, 2005), xxi.
[38] Gonzales et al., *Network-Centric Warfare Case Study*, 58.
[39] Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 144.

basic orders and information between units. Today's battlefield is much different. During Operation Iraqi Freedom, Major General Buford Blount credited BFT for allowing him to command a 200-230 kilometer front effectively.[40] The military relies on cyberspace to expand its span of control.

In addition to enhanced C2 capabilities provided by cyberspace, collaboration across organizational lines is also now feasible. Pilots providing close air support can communicate not only via radio but through instant messaging. Doing so allows the pilot, the ground unit, and the command elements to collaborate.[41] If needed, and if available, an intelligence analyst viewing ISR feeds can also assist in the targeting decision.[42]

Presumably, these new abilities change the organization of the military. The Goldwater-Nichols Act pushed the military to operate jointly. The latest trend extends the joint concept to a whole-of-government approach. In order to operate cohesively, all parties must be able to share information to synchronize their effects. Organization collaboration levies a requirement to use cyberspace effectively.[43]

Smaller, Cheaper Force

A force that uses cyberspace to be more effective ultimately means a smaller force can accomplish the tasks that used to take a larger one. The oft-cited example of how precision munitions now allow a single aircraft can service a target that used to take an entire squadron of World War II aircraft is analogous to what today's military can do with the superior information. A smaller force requires fewer ships and aircraft to deploy it and requires less effort and resources to sustain it. By requiring less force and fewer resources, military forces can be used in more places and require less preparation time to employ. Policy makers are afforded more options.

---

[40] Neil Baumgardner, "3rd Infantry Division Commander Praises C2V, Communications during OIF," *Defense Daily* 218, no. 34 (16 May 2003): 1.
[41] Examples of command elements include the Combined Air Operations Center or the Air Support Operations Center.
[42] Brian A. Eovito, "The Impact of Synchronous Text-Based Chat on Military Command and Control" (paper presented at the 11th Information Command and Control Technology Symposia, Cambridge, UK, September 2006), 69-70.
[43] David E. Johnson and Steve Pettit, "Principles of the Defense for Cyber Networks: An Executive Overview," *Defense Concepts* 4, no. 4 (Winter 2010): 16.

Furthermore, a smaller force costs less. The United States government currently is $15.36 trillion in debt (100.5% of GDP).[44] Starting in 2013, the military budget will be cut by $487 billion over 10 years.[45] However, even with the cuts, the government will incur another $3 trillion of debt over this timeframe.[46] Cost has always been a factor in strategy, but given the financial constraints of the foreseeable future, cyberspace's ability to squeeze out as much combat power from a limited number of platforms becomes crucial.

Deploying Fewer Resources

A related benefit of cyberspace is the ability to deploy military power while leaving people and resources at home. The use of the Predator is an example of how cyberspace can be used to limit the number of people who must be forward deployed. Operators "fly" Predator missions from the United States via terrestrial and satellite links to the aircraft. Raw, real-time footage can be streamed to a variety of locations both inside and outside the combat area. Intelligence analysts in the United States can store the video to analyze it in greater depth. By keeping intelligence analysts and the majority of the operators at home, fewer people are at put at risk and less logistical support is required.[47] This reduced forward presence lessens the political impact of having large numbers of US troops on foreign soil.

Cyberspace also gives the capability to process information faster and to make linkages teams of humans would not be able to make in a reasonable amount of time. Google retrieves websites across the web, indexes them, and uses a proprietary algorithm

---

[44] Bureau of Economic Analysis, "National Income and Product Accounts: Gross Domestic Product, 4th Quarter and Annual 2011 (Advance Estimate)," 27 January 2012, http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm (accessed 23 January 2012). Congressional Budget Office, "Budget Projections," Table 1-1, http://www.cbo.gov/ftpdocs/126xx/doc12699/BudgetProjections.xls (accessed 23 January 2012).

[45] Nathan Hodge, Julian E. Barnes, and Adam Entous, "Pentagon Unveils Spending Plan for Fiscal 2013," *Wall Street Journal Online*, 26 January 2012, http://online.wsj.com/article/BT-CO-20120126-714664.html (accessed 26 January 2012).

[46] Bureau of the Public Debt, "Monthly Statement of the Public Debt of the United States," 31 January 2012, http://www.treasurydirect.gov/govt/reports/pd/mspd/2012/opds012012.pdf (accessed 31 January 2012).

[47] United States Air Force, "Predator Combat Air Patrols Double in 1 Year," 6 May 2008, http://www.af.mil/news/story.asp?id=123097395 (accessed 23 January 2012). The Air Force claims that its remote split operations concept of flying UAVs reduces the number of people who have to be forward deployed. Thus, fewer people have to be housed, fed, protected, etc.

to rank the results—all within about a quarter of second.[48] The Google software, including its proprietary algorithm, forms the basis for the intelligence community's search applications allowing analysts speedy retrieval of intelligence information. Likewise, the intelligence community provides Intellipedia, essentially Wikipedia with intelligence information.[49] These tools proved their worth when they were primary means to create the National Intelligence Estimate on Nigeria, a process that included both information discovery and collaboration among Nigerian specialists and analysts from other specialties.[50]

Inter-Command Benefits

Cyberspace offers the functional combatant commands and the combat support agencies the ability to anticipate support requirements.[51] Whether through real-time reporting or via collaborative tools, organizations such US Transportation Command (USTRANSCOM), Defense Logistics Agency, US Strategic Command, US Cyber Command, the Intelligence Community, the State Department, or host of other organizations can prepare to support the tactical and operational fight. Ideally, this approach decreases latency for logistical items and intelligence collection. One idea is to develop a deployment common operating picture that would provide better visibility of deploying units. This approach promises to allow for the rapid re-tasking of units and better management of scarce USTRANSCOM assets.[52]

Cyberspace is a Reflection of Society

The use of cyberspace has become ubiquitous in Western society. The military, as a reflection of its nation's society, cannot escape from the benefits and trappings of this phenomenon. The societal shift towards standard information and communications technologies has spillover effects for the military. Boeing's use of computer-aided design (CAD) software allows them to manufacture planes more inexpensively.[53] Moreover,

---

[48] Google, "Technology Overview," http://www.google.com/about/corporate/company/tech.html (accessed 23 January 2012).
[49] Wilson P. Dizzard III, "Spy Agencies Adapt Social Software, Federated Search Tools," *Government Computer News*, 22 September 2006, http://gcn.com/articles/2006/09/22/spy-agencies-adapt-social-software-federated-search-tools.aspx.
[50] Bruce Finley, "Intelligence Fixes Floated at Conference," *Denver Post*, 22 August 2006, http://www.denverpost.com/search/ci_4216851.
[51] John B. Tisserand, III, *Network-centric Warfare Case Study*, 17.
[52] John B. Tisserand, III, *Network-centric Warfare Case Study*, 17.
[53] Starr, "Towards an Evolving Theory of Cyberspace," 36.

systems ranging from banking to commercial air conditioning to nuclear power plants now use the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol as the basis for their communications.[54] Military systems are also converting. For instance, Link-16 components incorporate TCP/IP, and it is the primary method for displaying data back to the air operations center.[55]

Cyberspace also enables a host of non-combat functions. Cyber-enabled business practices in the DOD include:

- commercial transactions with contractors
- payroll
- distributed research and development
- solicitation for goods and services
- health records
- personnel records[56]

The combination of these processes and others allow support entities to facilitate the smooth operation of the military enterprise.

Limits of Cyberspace

Cyberspace is, of course, no panacea. It can be a force multiplier, but it is not a substitute for traditional military force. The arduous stabilization phases of the conflicts in Iraq and Afghanistan showed the value of mass and persistence. Information, no matter how good, cannot put someone on every corner.

Moreover, with capability comes vulnerability. Improved situational awareness is not absolute situational awareness and does not give commanders absolute knowledge, nor is it without cost. Martin van Creveld describes the concept of an undirected telescope, where a person believes he has a good understanding of a situation but is really only looking at a small piece of a bigger scenario.[57] During Operation Anaconda, the Combined Air Operations Center (CAOC) overrode requests to provide close air support

---

[54] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Potomac Books: Dulles, VA, 2009), 184.
[55] Department of the Air Force, *Report on Defending and Operating in a Contested Cyber Domain*, SAB-TR-08-01 (Washington, DC: United States Air Force Scientific Advisory Board, 31 August 2008), 44.
[56] Department of the Army, *Critical Infrastructure Threats and Terrorism,* DCSINT Handbook no. 1.02 (Ft Leavenworth, KS: Training and Doctrine Command, 15 August 2005), IV-1.
[57] Van Creveld, *Command in War*, 257.

for troops in contact with the enemy. Instead, they diverted aircraft to strike a pickup truck displayed on a Predator feed. Presumably, the CAOC was operating based on its incomplete situational awareness (i.e., Predator feed) and did not have knowledge of the requests for immediate close air support.[58] Cyber technologies can fall prey to undirected telescopes and are not by themselves a substitute for good command.

Furthermore, situational awareness comes with a cost. In Operation Iraqi Freedom, the bandwidth per soldier increased by a factor of 50 over that from Operation Desert Storm.[59] This phenomenon serves as a warning for future conflicts, and the increased bandwidth requirements undoubtedly will cause physical chokepoints—satellites, undersea fiber-optic cables, and other key nodes. A deployment of a large force can quickly saturate the telecommunications infrastructure, leaving little margin for unforeseen problems or enemy action.

Moreover, new tools do not necessarily yield greater utility. A study of the use of collaboration tools used by air battle managers found mixed results. While the tools helped the air battle managers in some situations, they hindered them in others. Researchers posited that the addition of new tools—a luxury when tasks were light—presented a "tyranny of choice" when task demand was heavy.[60]

The deluge of data means information overload is quite possible, even with the tools that are supposed to manage information. David Lonsdale contends the advent of cyber technologies may not lift the fog of war but rather may thicken it or, worse yet, paralyze commanders waiting for perfect information.[61] Cyber tools that help process information are only as good as the validity of the assumptions with which they are programmed. If the original assumptions are faulty or the environment has changed, the data will be processed perfectly wrong. In short, friction can never be eliminated.[62]

---

[58] HQ AF/XOL, Operation Anaconda: An Air Power Perspective, staff study, 7 February 2005, 69-70.
[59] House, *Cyber-Terrorism Hearings before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services*, 108th Cong., 1st sess., 24 July 2003, Statement by Major General James D. Bryan, www.dod.mil/dodgc/olc/docs/test03-07-24Bryan.doc.
[60] Adam J. Strang et al., "Collaboration Technologies Improve Performance and Communication in Air Battle Management," *Military Psychology* 23, no 4. (2011): 404-405.
[61] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 58.
[62] Lonsdale, *The Nature of War in the Information Age*, 77-78.

The human is both a part of the system and is a vulnerability. Humans sometimes program cyber assets incorrectly. People also make mistakes as operators. Deputy Secretary of Defense Lynn publically admitted that a foreign intelligence service inserted code that was spread via a flash drive and infected classified networks that were supposedly “air gapped;” that is, they were not interconnected but required a human to transfer data from one network to another.[63] Presumably, the person who originally transferred the virus to a classified network was not intentionally trying to commit espionage, but this incident shows how mistakes can happen and can cause disproportionate consequences.

A primary limitation of any cyber system is the level of trust the human has in the system. It is possible to have either too much or too little trust in a cyber system. With too much trust, operators become too dependent on the system and fall victim when it fails. They can no longer accomplish the task in a different manner. Conversely, if the user does not have enough trust in the system, he loses the benefits cyberspace can provide. The degree of trust one should place in the system should be consummate with the realistic reliability in the system.[64]

The German and Allied use of cryptography during World War II illustrates this concept. The German military placed enormous faith in Enigma’s ability to keep its communications secure. Instead of critically assessing strengths and weaknesses of the system, the military continued to operate under the false assumption that nothing could go wrong. In contrast, the Allies only trusted their ability to securely pass intercepted German communications up to a point. Understandably, the Allies were afraid the Germans may capture intercepted information and realize that the Enigma had been compromised. As a result, the Allies only disseminated intelligence that could have been plausibly obtained by another source (e.g., from prisoners of war, direction finding, or a reconnaissance patrol).[65] The Allies sacrificed some intelligence obtained from Enigma intercepts (i.e., the information that could not be plausibly obtained by other means) to

---

[63] William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs* 89, no.5 (September/October 2010): 97.
[64] Department of the Air Force, *Report on Implications of Cyber Warfare, Volume 2: Final Report*, SAB-TR-07-02 (Washington DC: Air Force Scientific Advisory Board, August 2007), 52-54.
[65] R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, UK: Cambridge University Press, 2006), 4-9.

compensate for a system that was less than perfectly reliable. Yet, they were able to have enough trust in the system to exploit valuable intelligence.

The exploitation of the Enigma demonstrates a reliance on technology. The Germans not only trusted the Enigma to keep their communications secure, they relied on it. The Germans' arrogance of their ability to secure their communications blinded them from their vulnerabilities.[66] In the end, their overreliance on a single system ultimately had disproportionate consequences.

Summary

The value of cyberspace is in the missions that it enables. Modern society and, indeed, the modern American military rely on cyberspace and information to such a degree that reversion to a time without it is incomprehensible. The theoretical concepts of Metcalf's Law and network-centric warfare base cyberspace's value on various factors—the number of connections, the ability to collaborate, etc. The connectivity and collaboration cyberspace—if it presents timely information in a usable format—helps produce better information. Sun Tzu, the ancient Chinese military philosopher, wrote, "Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril."[67] Cyberspace gives the military the opportunity to understand itself and the enemy better.

Military operations in Iraq and Afghanistan provided excellent case studies to support Sun Tzu's assertion. The United States deployed a relatively small force that quickly defeated foes on their home turf. They did so, in large part, as a result of precision, superior information, and the ability to synchronize diverse military capabilities. It is counterfactual to analyze how these conflicts would have unfolded without unfettered access to cyberspace. However, it is not much of a stretch to suggest that the military would have had to make major changes—changes that it would not have wanted to make—if cyberspace was unavailable of if it could no longer use its cyber systems.

---

[66] Ratcliff, *Delusions of Intelligence*, 232.
[67] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 2005), 125.

In fact, the modern military is integrally tied to cyberspace. Whether a Stryker Brigade Combat Team or a Link-16 equipped aircraft, modern military platforms cannot separate cyber capabilities from its primary mission. Furthermore, the impending budget cuts will likely necessitate a smaller force structure. Each platform will have an expectation to do more. One such method is to link the platforms to leverage others' capabilities. Furthermore, the ability to link dynamically and to self-synchronize offers a high degree of flexibility. In a complex environment, this ability gives the military more options.

Cyberspace cannot solve every need, and it does have potential downsides. First, cyberspace can only partially replace mass. Cyber technologies can assist in providing precision, which reduces some of the need for mass, and they probably succeed in assisting commanders to make faster decisions on how best to utilize force. However, cyberspace cannot provide presence. In counterinsurgencies or stability operations, securing an area still requires mass.

A second major drawback of cyberspace is the human user. Over time, the technology that drives computers increases its capabilities to process information. The human user, on the other hand, cannot realistically increase its capacity. Too much information can result in information overload. Aside from information overload, cyber tools can become a crutch, and its users can become overly reliant on these systems. Furthermore, users may become addicted to the quality of information and subsequently delay action until it is received. If so, the cyber systems inhibit decision making rather than facilitating it.

A third potential downside is integrating with allies and among the US military services. Although the Australians see cyber integration as valuable and have invested in operating with US forces, it is unlikely that all of our allies will pursue such a path. For that matter, predicting who will be allied with the US in the next conflict is extraordinarily difficult. We may be able to plan to integrate with our closest friends, who happen to be technologically advanced nations, but we cannot possibly integrate with every possible ally for both political and technological reasons. Even integration and interoperability among the US military services has had several roadblocks. The Army and Marine Corps BFT systems did not communicate with each other in the major

combat operations phase of Operation Iraqi Freedom.[68] Planning and foresight can alleviate some of the problems between the services and between allies but not all of them.

Despite the downsides, one cannot overlook the upsides cyberspace provides. The United States military is tied to technology including cyber technologies. It is one of the asymmetric advantages the military has used against its enemies. The United States military is not the United States military without cyberspace.

[68] Imad Bitar and Brian L. Felsman, "Blue Force Tracking in Operation Enduring and Iraqi Freedom," *Technology Review Journal* 13, no. 2 (Fall/Winter 2005): 81-83.

CHAPTER 3

CYBER WARFARE CHARACTERISTICS AND EFFECTS

Chapter 2 analyzed the military benefits of cyberspace. This chapter examines the risks posed by hostile cyber attacks. It seeks to explain the harm others can impose on military operations. Only after weighing the benefits and the risks can the military determine how much effort and resources to apply to resolve any residual risks.

As the United States' military relies more on cyberspace, others are recognizing the dependence. They seek to neutralize the United States' military's asymmetric advantage it enjoys in cyberspace. This chapter examines the characteristics that make cyber warfare unique. It then looks at the effects cyber warfare can generate and the impact these effects have on strategy. The final section discusses an overview of cyber defense principles.

Characteristics of Cyber Warfare

Before one can understand cyber warfare, one must understand the environment in which it operates. Martin Libecki notes, "Cyberspace is its own medium with its own rules." As a man-made construct, cyberspace is the only domain in which the rules are both contrived and changeable. Libicki further points out, "Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities."[1] As such, cyber warfare can be analyzed using inductive and deductive reasoning.

On the other hand, cyber warfare is also in part an unknown. Cyber warfare has not been a tradition of warfare. Much like airpower at the beginning of World War I, militaries have not employed cyber warfare on a large scale. The principles and capabilities of cyber warfare are not derived from past military application but from its potential in future conflicts. Since historical military examples are not prevalent, criminal activity in cyberspace may offer a glimpse of cyber warfare's possibilities. Identity theft from the Internet disrupts the lives of its victims and causes businesses to distrust the identities of their customers. The Federal Trade Commission reported that Americans

---

[1] Martin C. Libicki *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), iii.

spent over 25 million hours recovering from identity theft, and some still cannot trust that they have fully repaired the damage.[2] Moreover, the CIA claims criminal groups operating outside of the United States have broken into utility companies' systems and have extorted payments to prevent a shutdown.[3] More tangibly, in 2000, a prospective employee who did not get a job at an Australian sewage treatment plant retaliated by using a cyber attack to dump thousands of gallons of raw sewage.[4] Criminals have shown that disruptive and destructive attacks are more than just theoretically possible. They have also shown a degree of creativity in their tactics. An entire industry devoted to cyber security has developed to stay ahead of the criminals. Although the industry is heavily geared toward protective measures, its size, specialization, and in some regards, its very existence points toward the need to be resilient against criminals. The military should expect the creativity and cunning criminal organizations to carry over to states as well.

History of Cyber Warfare

Examples of actual cyber warfare are rare. The Estonians assumed the Russian government initiated attacks on Estonia after the relocation of a controversial statue, but later, the Estonians arrested one of its citizens for perpetrating the attacks.[5] The degree of actual Russian government involvement, if any, is not clear.

Russia's conflict with Georgia may have been the first case study of coordinated major military operations with cyber warfare.[6] Prior to the invasion, Georgia experienced denial-of-service attacks against government and military communications systems as well as against Georgian news agencies.[7] Russia's purported objectives of the attack were threefold. First, it wanted to disrupt the Georgian government's ability to command and control its military forces. Second, it wanted to sow fear and discontent among the

---

[2] Federal Trade Commission, "FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005," http://www.ftc.gov/opa/2007/11/idtheft.shtm (accessed 15 March 2012).

[3] Clay Wilson, "Cyber Crime," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 433.

[4] Briefing, MITRE Corporation, subject: Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia, August 2008.

[5] BBC News, "Estonia Fines Man for 'Cyber War,'" 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.

[6] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, 6 January 2011, 2, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[7] Hollis, "Cyberwar Case Study," 6.

Georgian population.[8] Third, the Russians wanted to demonstrate their ability to strike the Baku-Ceylon pipeline. They demonstrated this ability by using airstrikes to strike near the pipeline but intentionally did not hit it. Simultaneously, cyber attacks demonstrated the ability to shut down the pipeline via cyber means without actually doing so.[9]

The Russian military did not initiate the cyber attacks—at least not directly. Rather, the attacks had links to the organized crime group, the Russian Business Network. Yet, sufficient evidence exists to suggest the Russia government not only condoned the Russian Business Network's participation but probably sponsored it. For example, the propaganda present on the Georgian government's hacked websites contained sophisticated, high-quality graphics that realistically only could have been accomplished prior to the start of hostilities.[10] Future conflicts may include a mix of state-controlled cyber attacks with state-condoned or state-inspired cyber attacks. The military must consider scenarios with diverse actors when analyzing the operating environment and the cyber component of the environment.

Perhaps the most interesting example of a potential cyber warfare attack involves a worm named Stuxnet and an Iranian nuclear facility. Stuxnet spread throughout the world but only affected Siemens-manufactured industrial control systems that ran a very specific configuration, the configuration used at Iranian uranium enrichment facilities.[11] The worm caused the Iranian centrifuges to spin outside of its normal operating parameters despite showing normal readings to technicians.[12] The result, according to a *New York Times* report, is a multiyear delay in the Iranian nuclear program. The United

---

[8] Richard M. Crowell, "War in the Information Age: A Primer for Cyberspace Operations in the 21st Century," (Newport, RI: Naval War College, 2010), 14.

[9] Hollis, "Cyberwar Case Study," 4-5.

[10] Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, 2010), 97-99.

[11] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all.

[12] Nicholas Falliere, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier," version 1.4 (February 2011). Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Sources differ on the exact nature of the effects on the centrifuges. Broad et al. claim that Stuxnet caused the centrifuges to spin "wildly out of control." Falliere et al., "W32.Stuxnet Dossier," pg. 43, describes the virus causing programmable logic controllers to change speeds at programmed intervals. What is clear is that Stuxnet caused the centrifuge to operate outside of its recommended operating parameters and that the operators received readings falsely indicating normal operation.

States and/or Israeli governments are reported suspects, but neither admits any involvement.[13] Although Stuxnet is not an example of cyber warfare against another military, it shows the degree in which cyber attacks can impact objects of value in international politics.

Relation to Traditional Military Capabilities

An adversary can employ various methods of cyber attacks. The cyber-based methods are not unlike other military capabilities. For instance, a basic concept of maneuver warfare is to bypass the enemy's strengths in order to strike at his vulnerabilities. Cyber attacks are no different—at either the strategic level or the tactical level.[14] At the strategic level, cyber attacks prey on the militaries that are dependent on cyberspace for their combat effectiveness. Cyber warfare limits a military's full combat potential much as the Turkish Parliament's decision to deny the US Army access to Turkish territory during the Operation Iraqi Freedom limited combat potential. Tactically, a multitude of different attacks can induce a variety of outcomes, many of which are similar to traditional tactics. For example, denial-of-service attacks are much like electronic jamming.[15] Probing occurs both in cyber warfare and in the traditional domains. Cyber attacks that simply intend to induce a reaction and to require spending time to clean up the damage are not unlike other diversionary attacks. Just as in traditional warfare, tactics are diverse. Pigeonholing cyberspace into a set of narrow, preconceived nations is dangerous, because practitioners lose the ability to imagine the possibilities of cyber warfare.

Cyber Geography

Cyberspace is not bound by traditional geography; rather, cyberspace has its own geography. Cyber geography consists of both physical and logical components. While the stereotype of cyber warfare is a bunch of geeks operating from some remotely located internet connection, not all attacks can be executed remotely. Some attacks require the attacker to operate "in the line-of-sight of radio networks and closed battlefield command

---

[13] Broad et al., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[14] Billy K. Rios, "Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Amsterdam: Ios Press, 2009), 144.

[15] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009), 171.

networks, in the footprint of satellites, with human-enabled access, or within the range of future, high-powered, energy wave devices."[16] A "candy drop" is a technique where an agent leaves a flash drive or a similar device infected with malicious code at a location where the target might use it.[17] Another example of an attack that requires specific access is when an EC-130H Compass Call electronic warfare aircraft took over an Iraqi tactical radio network.[18] Physical access can matter with cyber attacks. On the other hand, many other types of attacks can use interconnected computer systems to launch attacks from anywhere on the planet.

At the physical level, cyber infrastructures have chokepoints, including undersea cables, satellites, and "cyber hotels"—locations where large numbers of fiber-optic cables converge.[19] Dr. Kamal Jabbour of the Air Force Research Labs claims physical control of cyberspace infrastructure allows for the control of information passing through it.[20] Many of the most critical systems require physical access to exploit them, since their operators take measures to mitigate inadvertent or intentional disruptions from external connections.[21]

Cyber geography also has a non-physical component. Logically, data can reside anywhere and move dynamically. Many of Wall Street's computers for electronic trading were physically located in the World Trade Center. Fortunately, the 9/11 attacks did not impact the trades since another server mirroring the data was located across the street.[22] However, this server could have just as easily been in another state or another country. Facebook randomly assigns data to a data center.[23] Facebook users do not know and

---

[16] Forest B. Hare and Glenn Zimmerman, "The Air Force in Cyberspace: Five Myths of Cyberspace Superiority," in *Military Perspectives on Cyberspace*, ed. Larry K. Wentz, Charles L. Barry, and Stuart H. Starr (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009), 88.
[17] Stiennon, *Surviving Cyber War*, 8.
[18] Patrick D. Allen, *Information Operations Planning* (Norwood, MA: Artech House, 2007), 10.
[19] Gregory J. Rattray, "An Environmental Approach to Cyberpower," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 259; Stuart H. Starr, "Toward a Preliminary Theory of Cyberspace," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 58.
[20] John W. Gloystein, "Cyberdeterrence in 2035," (Research paper, Air War College, February 2010), 7.
[21] Libicki, *Cyberdeterrence and Cyberwar*, 18-19.
[22] Allen, *Information Operations Planning*, 32.
[23] Jeff Rothschild, "High Performance at Massive Scale – Lessons Learned at Facebook." Address. University of California, San Diego, 8 October 2009.

probably do not care where their data is stored. Their data may move and the route it takes may change with a flip of the switch or a change in the code. The logical geography of cyberspace differs from other forms of warfare.

The code that runs software and hardware is also an important component of cyber geography. A system is only vulnerable when a developer writes code with errors, which causes the program to do something unintended. If there are vulnerabilities in the code, they only last as long as the time a developer can fix them and deploy the patch. This concept generates a race between the developer and the attacker. A great attack tool today may be obsolete tomorrow. [24]

The lines between the physical and logical layers begin to blur when the concept of sovereignty is introduced. The utopian's vision is that the Internet is a global commons for the good of all. The reality is the Internet consists of globally connected private and government-owned networks.[25] The concept of who owns what and who controls what is a complicated matter. Clearly, a state can assert sovereignty over physical assets within its boundaries, but the sovereignty afforded over the information residing on that physical infrastructure is less certain. What if the information is transitory? What if it resides in multiple locations? What responsibility does the sovereign have to protect the information that resides on machines within its borders? What responsibility does it have for the information on these machines? If an al Qaeda recruiting site resides on a server in Indonesia, does Indonesia risks being labeled as harboring terrorism? Does it matter if the information is mirrored from a server residing in Pakistan or if the server is part of a "cloud"? Does the sovereign even have realistic means to police such information? Many of these questions remain unanswered.

Early Warning and Detection

Another aspect of the cyber environment is the speed in which cyber attacks occur coupled with the ability for attacker to hide in cyberspace. These traits make early warning extremely difficult. The first indication of an attack may be when the victim perceives he is under attack.[26]

---

[24] Libicki, *Cyberdeterrence and Cyberwar*, xiv.
[25] "Cyberwar," *Economist* 396, no. 8689 (3 July 2010): 12.
[26] Libicki, *Cyberdeterrence and Cyberwar*, 62.

Viruses tend to be indiscriminate. They are part of the noise of cyberspace. Other attacks are much more focused. A targeted attack takes a great deal of intelligence. The attacker must collect specific information about a system's configuration and its vulnerabilities. Today's probe may be tomorrow's attack vector. Analyzing seemingly innocuous information and probes is one approach to determine if an attack is pending and to resolve any vulnerabilities. However, the level of noise on many networks makes this an arduous, if not an impossible, task. At present, the cyber environment lacks reliable early warning of attack.

Redistribution of Power

Cyber warfare threatens to alter the distribution of power. Cyber warfare is relatively cheap. A research lab can find vulnerabilities in routing software and other common network components for $3-20 thousand.[27] The exercise "Dark Angel" proved that with $500 million and 3 years' time, an adversary could launch devastating attacks against United States infrastructure and degrade the military's ability to project force.[28]

States and non-state entities also gain operational reach and standoff capabilities with cyber warfare. States that cannot afford blue-water navies or offensive land and air forces can afford a cyber warfare capability. More troubling, terrorists and other non-state actors can afford many of the same capabilities.[29]

Third parties—either acting as a proxy for a belligerent or acting on their own—now have the ability to intervene using cyber warfare. Sympathizers of all sides launched cyber attacks following the EP-3 AIRES II crash landing on Hainan Island and during the Israeli-Palestinian conflict. In these cases, the impacts of the attacks were little more than a nuisance.[30] However, the use of 3rd parties in other conflicts has had more significant consequences. The 2008 Russian-Georgian War involved cyber attacks against Georgian government and military systems. Some attacks originated from "patriotic Russian

---

[27] Skoudis, "Information Security Issues in Cyberspace," 183.

[28] House. *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security*. 105th Cong., 1st sess., 25 April 2007.

[29] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, Franklin P. Kramer, Stuart H. Starr, and Larry K. Wentz, eds. (Dulles, VA: Penguin Books, 2009), 316.

[30] Allen, *Information Operations Planning*, 8-9.

hackers". Based on Russia's previous conflicts with other former Soviet states, these "patriotic hackers" were probably "crowd-sourced" by Russian agents. Crowd sourcing is a method where a sympathetic group of people are given a generic task. In the case of the Russian-Georgian conflict, a group of hackers launched distributed denial-of-service attacks against government systems soon after the initiation of hostilities.[31] The United States' military is likely to encounter third-party hackers in future conflicts —either outsourced (or crowd-sourced) by the adversary or who operate independently.

The Threat Within

Insiders are similar to the third-party problem. An insider's motivation to conduct an attack can stem from being a covert saboteur to a disgruntled employee to plain incompetence. Due to the level of trust and access, insiders can cause significant damage and pose a daunting problem for any organization. The Wikileaks incident, for example, involved a relatively low-level soldier, PFC Bradley Manning, whose damage, while serious, could have been even more extensive.[32] If working with a foreign intelligence service instead of an open-government advocate, Manning may have been able to pass classified information undetected for quite some time, or he could have turned his anger and access into sabotage and altered or destroyed data on classified systems.

The insider need not be a member of a military organization. The insider may be situated in any part of the supply chain. As mentioned earlier, a cyber attack can only occur if there is a vulnerability in the code. Yet, the vulnerability does not necessarily have to be an accident. The programmer may intentionally leave a vulnerability that can be exploited later. Much of the software the military uses is commercially available, and much of it is produced—at least in part—in foreign locations.[33] The United States has reason to fear supply chain attacks, since it used them against the Iraqis in Operation Desert Storm. The United States' military derived the locations of computers belonging to military units based on the tags from computers exported to Iraq from the United

---

[31] Stiennon, *Surviving Cyber War*, 75-76. Similar incidents occurred during heightened diplomatic tension between Russia and Estonia, Lithuania, and the Ukraine in 2007, as well as with Kyrgyzstan in 2009.
[32] See Ed Caesar, "Bradley Manning: Wikileaker," *The Sunday Times*, 19 December 2010, http://www.edcaesar.co.uk/article.php?article_id=53 (accessed 30 April 2012) for background on Manning's motivations. Manning believed the world should have access to the information he released.
[33] John M. Weinstein, "Ten Reasons Why Nuclear Deterrence Could Fail: The Case for Reassessing US Nuclear Policies and Plans," in *Deterrence for the 21st Century*, ed. Max G. Manwaring (Portland, OR: Frank Cass, 2001), 31-32.

States.[34] The military sees the threat from insiders and the supply chain and believes small-scale threats from these groups can lead to disproportionate consequences.[35]

Is Defense the Stronger Form of Warfare in Cyberspace?

Another characteristic of cyber warfare is the question of whether the offensive is superior to the defensive. Clausewitz asserts that "the defensive form of warfare is intrinsically stronger than the offensive."[36] Defenders have the advantage of terrain and, if defending home territory, intimate knowledge of the land, infrastructure, and population. Some question whether the Clausewitzian advantage of the defensive applies in cyberspace. This question holds particular relevance in terms of guaranteeing mission assurance in the face of cyber attacks. If cyber defense is truly weaker, then it is a foolish waste of resources to attempt to defend cyberspace.

As opposed to traditional warfare where the defender has the advantage in terms of required active and passive resources, one perspective claims deploying defensive cyber measures costs far more than the corresponding offensive cyber weapons, further shifting power to those with the capability to attack.[37] The attacker only has to focus on a particular vulnerability; whereas, the defender must concern himself with a host of possible attacks. From this perspective, the cost advantage clearly goes to the attacker.

However, once the attacker uses a particular exploit, he faces a high probability of its discovery. Once discovered, an attacker can analyze the attack tool and develop countermeasures. Once the countermeasures are employed, the attack tool's residual utility is limited to those systems that fail to apply the countermeasures or misapply them. If a vulnerability was found at little cost or if the tool yielded a great deal of military value, then the loss of a particular attack tool is of little concern. However, if the attacker knows of only a few vulnerabilities in which he can exploit, the loss of an attack tool greatly diminishes his capacity for cyber attacks. The defender has the advantage of having a defensive infrastructure in which he only has to add a particular countermeasure.

---

[34] Allen, *Information Operations Planning*, 6.

[35] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Office of the Secretary of Defense, July 2011), 3.

[36] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 358.

[37] Huba Wass de Czege, "Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack," *Military Review*, July-August 2010, 92.

The attacker has to start over. From this perspective, the net cost advantage favors the defender. As long as the attacker does not have an arsenal of vulnerabilities to exploit, he must take a measured approach and must factor in opportunity cost.

Another common advantage attributed to the attacker is the notion that attacks can occur at the speed of light.[38] A fundamental advantage of any military attack is the ability to take the initiative. Clausewitz recognized this relationship between attack and defense. "[D]efense has a passive purpose: *preservation*; and attack a positive one: *conquest*. The latter increases one's own capacity to wage war; the former does not."[39] Cyber attacks can occur without warning, which increases the readiness requirements for the defense. However, the defense can also operate at the speed of light to implement countermeasures. The lag time between the attack and the application of countermeasures is the attacker's primary temporal advantage. Cyber attacks inherently offer the advantage of surprise to a degree Clausewitz could not imagine. However, the defenders can also negate a cyber weapon quickly.

Traditional analogies of defense are applicable to other aspects of cyber warfare. Defensive fortifications enhance the defense's ability to repel an attack. They increase costs for the attacker, but they are not impenetrable. Improper defensive fortifications or excessive defenses can be disadvantageous. The Maginot Line is a historical example of this. Cyber defenses are no different. They must be deployed in a logical and reasonable manner.

Cyber defense—as with other forms of warfare—is the stronger form of warfare, but its strength is not absolute. As Clausewitz argued, the defensive form of warfare is stronger but is only used by those in a position of weakness.[40] Once the defender gains an advantage, he must counterattack. The means of counterattack are unimportant. The concept of mission assurance is to preserve the ability to maintain the initiative to achieve political objectives.

---

[38] Wass de Czege, "Warfare by Internet," 92.
[39] Clausewitz, *On War*, 358 [emphasis in original].
[40] Clausewitz, *On War*, 358.

Cyber Warfare Effects

Fundamentally, cyber warfare can produce three primary effects. First, cyber attacks can cause damage or destroy physical assets. Many critical infrastructure devices rely on Supervisory Control and Data Acquisition (SCADA) and distributed control systems to automate and control tasks, including physical tasks. The Government Accountability Office warns of the catastrophic damage attacks on SCADA systems could impose (e.g. flooding from opening dams or loss of electrical power from overloading electric generators) and also warns that foreign governments or terrorists groups are capable of exploiting the vulnerabilities.[41] The Idaho National Labs demonstrated such a vulnerability in an experiment where a cyber attack caused a power plant generator to self-destruct, damage that would take months to fix.[42]

While the military only operates a limited number of traditional SCADA systems, mainly to support garrison infrastructure, its aircraft and satellite control networks are essentially SCADA systems. In 2008, a B-2 Spirit bomber crashed on takeoff when a sensor gave a faulty reading and caused the $1.4 billion aircraft to stall. Although the cause of the crash was due to moisture in the sensor, corrupting the aircraft's code to have the sensor pass faulty information to flight computer would have caused the same result.[43] While this may seem a bit far-fetched, scientists have successfully corrupted a car's computer to override brake controls and to shut down the engine.[44]

Furthermore, tampering with systems that control satellites in orbit could have catastrophic effects on the missions these satellites support. Unknown groups have hacked into US Geological Service and National Aeronautics and Space Administration (NASA) satellites. These attackers had the ability to issue commands that could have destroyed the satellite but did not do so.[45] Destroying military equipment by cyber attack

---

[41] Government Accountability Office, *Critical Infrastructure Protection: Challenges and Efforts to Control Systems*, GAO-04-354 (Washington, DC: Government Accountability Office, March 2004), 11.
[42] Jeanne Meserve, "Mouse Click Could Plunge a City into Darkness, Experts Say," *CNN.com*, 27 September 2007. http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US.
[43] Michael Sirak and Marc Schanz, "Air Force World," *Air Force Magazine* 91, no. 7 (July 2008): 16.
[44] Rebecca Boyle, "Proof-of-Concept CarShark Software Hacks Car Computers, Shutting Down Brakes, Engines, and More," *Popsci.com*, 14 May 2010, http://www.popsci.com/cars/article/2010-05/researchers-hack-car-computers-shutting-down-brakes-engine-and-more (accessed 4 April 2012).
[45] Debra Werner, "Satellite Security: Hacking Cases Draw Attention to Satcom Vulnerabilities," *C4ISR Journal* 11, no. 1 (January/February 2012): 16.

would take a great deal of intelligence, access, and luck. However, if successful, the results could be significant.

The second major effect cyber warfare can create is disruption. Denial of service attacks against key nodes is much like an electronic warfare platform jamming a radio channel.[46] Other forms of disruption include deleting files. These disruptive activities are not persistent. Network defenders can mitigate denial of service attacks, and files can be restored from backup tapes. Destroying information is difficult, if not impossible. In many cases, attacks do not have to persist. The jamming (electronic or cyber) of a key radar site needs only to last long enough for a strike package of aircraft to move to their target. Disruption enhances the effectiveness of other actions.

The third major effect of cyber warfare is the ability to cause an adversary to lose confidence in its information. Cyber attacks have the capacity to produce what Clausewitz described as the fog of war. The Allies went to great lengths to deceive the Germans of the actual location of the landing in France, which ultimately put the German military in a more disadvantageous position.[47] More recently, the Serbian military transmitted false radio messages it knew NATO would intercept. The Serbs intended to frustrate NATO's targeting and divert its resources.[48] Cyberspace gives another medium to deceive the adversary and frustrate its command and control.[49]

Militaries that are more dependent on cyber technologies are hurt more from a loss in confidence in these technologies. False messages can be sent, or data could be surreptitiously altered.[50] An attacker could send parts and supplies to the wrong locations—an effect that would hamper the units requiring the supplies and would needlessly tie up transport assets. Once the user perceives the system does not produce accurate information, it is hard to return to a state of trust. With a disruptive attack, the

[46] Skoudis, "Information Security Issues," 171.
[47] James A. Lewis, "Thresholds for Cyberwar," Center for Strategic Studies Report (Washington, DC: Center for Strategic Studies, September 2010), 4-5.
[48] Allen, *Information Operations Planning*, 6.
[49] Detecting incidents where data is changed is much more difficult. While a user normally knows if a system crashes, he may not know if data is subtlety changed.
[50] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 114-116.

user typically knows when a system becomes available again; it is far more difficult for a user to determine when he is no longer being deceived.

The Israeli attack on the Syrian nuclear reactor shows how cyber attacks can both deceive and disrupt. The Israelis purportedly exploited the centralized nature of the Syrian integrated air defense network. They used cyber attacks and/or electronic jamming to deny use of key links. Cyber attacks also spoofed the command and control portion of the system to cause confusion. Of note, the cyber attacks originated from both ground-based computers and from attacking aircraft. The end result was the Israeli air force penetrated into the deepest parts of Syrian airspace and accomplished its mission without taking any losses.[51]

Cyber Warfare, Coercion, and Deterrence

The effects cyber attacks produce ultimately serve larger strategic goals. For the military, cyber defense seeks to maintain freedom of action in all of the military domains. (See chapter 2 for a full discussion of the military benefits of cyberspace). Cyber attacks seek to coerce the enemy. Against military targets, cyber attacks attempt to deny the enemy's full use of its military capabilities.[52]

Deterrence is the act of persuading an adversary not to do something it would otherwise do. Deterrence is, therefore, an act of coercion, since it is an indirect approach to influence another. At the same time, it is the inverse of coercion, since it seeks to counter another's coercive actions.[53] A strategy to deter cyber attacks against the military is difficult. It has limitations. It is likely to fail. However, it is a tool that can be used as part of the equation to obtain mission assurance.

---

[51] David A. Fulghum and Robert Wall, "U.S. Electronic Surveillance Monitored Israeli Attack on Syria," *Aviation Week*, 21 November 2007, http://www.aviationweek.com/aw/generic/story.jsp?id=news/ISRA112107.xml&headline=U.S.%20Electronic%20Surveillance%20Monitored%20Israeli%20Attack%20On%20Syria&channel=defense (accessed 21 February 2012).

[52] The focus on denial does not mean that cyber attacks cannot be used to punish a civilian population or, for that matter, any other means of coercion. Rather this this paper chooses to focus on the military aspects of cyberspace, which necessarily excludes the homeland security and law enforcement aspects that are handled by civilian entities.

[53] Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1998), 31.

The limits of cyber deterrence are prevalently stated in the literature. For one, attributing the source of the attack is difficult.[54] The introduction of third parties into the conflict gives belligerents plausible deniability. Moreover, those using cyber attacks can leave false evidence to shift blame to an innocent party.[55]

Aside from attribution, other factors make deterrence difficult. Unlike nuclear deterrence, a cyber attack does not violate a clear taboo.[56] A cyber attack prior to armed conflict may be an option short of war. After an armed conflict has begun, it is not a heinous escalation of hostilities as nuclear, biological, or chemical weapons are. Furthermore, the concept of counterforce in cyberspace is weak at best. Even if the target of a cyber attack can find the specific attacker, destroying the computer that perpetrated the attack yields little value.[57]

Despite the difficulties, deterring cyber warfare has value. The deterrence of terror groups is an appropriate analogy. Thom Shanker and Eric Schmitt argue that while a state cannot effectively threaten territory, it can deter terrorists in other ways. States can deter by threatening other items of value, including: glory, reputation, the ability to gain new recruits, and the probability of success.[58] The concept of resilience helps accomplish these deterrent goals. A failed attack undermines the aura of attacker and exposes the attacker to retaliation from diplomatic, economic, or military means.

Cyber Defense Principles and Characteristics

Much of the chapter to this point has focused on the offensive aspects of cyber warfare. This section explores the characteristics of cyber defense. It begins by exploring how passive and active defenses apply in cyberspace.

Passive Defense and Information Assurance

---

[54] For examples see F.G. Hoffman, *Homeland Security: A Comparative Strategies Approach* (Washington, DC: Center for Defense Information, March 2002), 55; Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 293-296; United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare, Volume 1: Executive Summary and Annotated Brief*, SAB-TR-07-02 (Washington DC: United States Air Force, August 2007), 23-24; The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, 12-15.

[55] Hoffman, *Homeland Security*, 59.

[56] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 293-296.

[57] Libicki, *Cyberdeterrence and Cyberwar*, xvi.

[58] Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret War against Al Qaeda* (New York: Times Books, 2011), 53.

Passive defense is the most basic form of defense. The DOD defines passive defense as "measures taken to reduce the probability of and minimize the effects of damage caused by hostile action without taking the initiative."[59] On land, passive defense may include defensive barriers or concertina wire. In cyberspace, passive defenses include the use of antivirus programs, firewalls, and security policies. These measures also fall under the rubric of information assurance, or "measures that protect information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation."[60] Passive defense and information assurance measures equate to preventative measures.

Active Defense

As its name implies, active defenses require a degree of affirmative action by the defender. Officially, active defense is defined as "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[61] What active defense exactly means in cyberspace is not clear. When a defender decides to take action in his own network, is he conducting an active defense? Does blocking a port on a friendly router constitute a counterattack? General Keith Alexander, Commander, USCYBERCOM, describes teams hunting for potential intrusions as a form of active defense.[62] His characterization suggests friendly action against an ongoing hostile action should be classified as active defense.

Although actions taken in one's own network fall into a gray area, actions taken outside of one's network clearly fall into the category of active defense. Furthermore, active defenses may also include kinetic actions. For example, an airstrike against a device that is jamming a communications satellite is a form of a counterattack against a hostile action contesting cyberspace. Active defenses that solely occur within cyberspace

[59] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 254.
[60] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 160.
[61] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2.
[62] Aliya Sternstein, "Defense Cyber Chief: The Cloud is the Military's Next Internet," *Nextgov.com*, 27 October 2011, http://www.nextgov.com/cloud-computing/2011/10/defense-cyber-chief-the-cloud-is-the-militarys-next-internet/50023/ (accessed 30 April 2012).

include blocking all traffic as close to the hostile computer as possible or using cyber counterattack to neutralize hostile threats.[63]

Counterattack has major limitations. To counterattack, the defender must know that he is actively under attack. The attack must be a disruptive, denial-of-service attack. Destructive or deceptive attacks generally lack an ongoing nature that would facilitate a return attack. Furthermore, counterattacks risk conflict escalation or attacks on innocent parties.[64] In 2007, Estonia was subjected to a distributed denial-of-service attack. Many of the attacking computers were coopted by hostile entities. If the Estonians would have counterattacked, they would have attacked innocent parties in Europe, China, and the United States among other place.[65] Much like deterrence, active defense has limitations in obtaining mission assurance. However, it has value in certain circumstances and should be part of the toolkit to ensure cyberspace is available.

The Role of Attribution

The problem of attribution, though vital to deterrence and response actions, only plays an ancillary role in resiliency. Attribution is important to execute some forms for active defense but also for some passive defenses. For example, on 14 August 2003 when the power went out across much of the northeastern section of the United States, Federal, military, and civilians leaders had to determine if the event—which would eventually cost $7-10 billion in damages—was cyber related and whether it was intentional.[66] If an event such as this is an accident, one only has to make sure a hostile entity does not find a way to exploit what is an obvious vulnerability. If it would have been intentional, the defender must identify and shore up vulnerabilities prior to another attack. As will be discussed in more detail in chapter 4, implementing immediate, non-cyber workarounds may be the best option, since the attacker may be capable of launching a similar attack against another target at any time until the vulnerability is patched. The need to know who did it is not as important as knowing how it was done and whether someone intended

[63] Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protecting Critical Infrastructure against Cyber Attacks* (New York: Oxford University Press, 2003).
[64] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 142-148.
[65] James R. Langevin et al., *Securing Cyberspace for the 44th Presidency,* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, (Washington, DC: Center for Strategic and International Studies, December 2008), 25-26.
[66] Michael Dumiak, "Casus Belli," *Defense Technology International* 4, no. 8 (1 September 2010): 31.

to do it. In this case, intelligence gathering may be more important than retaliation. To achieve resiliency, attribution data helps prevent further attacks.

Policy, Law, and Constraints

Legal and policy considerations are paramount when dealing with attribution and other aspects of cyber defense. The latest Department of Defense strategic guidance—*Sustaining US Global Leadership: Priorities for 21st Century Defense*—contains two cyber-related priorities for US armed forces. First, the military must project power despite anti-access and area denial challenges, which specifically includes weapons that deny cyberspace. Second, the military must operate effectively in space and cyberspace.[67] Each of these priorities places a heavy burden on the ability to fight through cyber attacks.

The US code defines the roles of each of the Services, but US code is silent on who fights in cyberspace. Instead, the Unified Command Plan gives the authority to fight in cyberspace to US Strategic Command, which it delegated to its sub-unified command—US Cyber Command (USCYBERCOM).[68] USCYBERCOM's mission includes "planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and…to ensure US and allied freedom of action in cyberspace, while denying the same to our adversaries."[69]

USCYBERCOM and its assigned forces are bound by international and domestic law. Article 2, paragraph 4 of the United Nations Charter defines actions that constitute the use of force and when the use of force is appropriate.[70] Specifically, the charter prohibits "the threat or use of force against the territorial integrity or political independence of any state, or in a manner inconsistent with the purpose of the United

[67] Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Office of the Secretary of Defense, January 2012), 4-5.
[68] Robert M. Gates, Secretary of Defense, to Secretaries of Military Departments; Chairman of the Joint Chiefs of Staff; Deputy Chief Management Officer; Commanders of the Combatant Commands; Assistant Secretaries of Defense; General Counsel of the Department of Defense; Director, Operational Test and Evaluation; Director, Cost Assessment and Program Evaluation; Inspector General of the Department of Defense; Assistants to the Secretary of Defense; Director, Administration and Management; Director, Net Assessment; Directors of the Defense Agencies; Directors of the DOD Field Activities, memorandum, 23 June 2009.
[69] U.S. Cyber Command Public Affairs, "U.S. Cyber Command," U.S. Strategic Command, December 2011, http://www.stratcom.mil/factsheets/cyber_command/ (accessed 14 March 2012).
[70] Starr, "Toward a Preliminary Theory of Cyberspace," 67.

Nations."[71] Legal experts widely interpret the charter to legitimize any activity short of violent force, since non-violent means are methods of solving conflict without war. Following this logic, cyber operations are only prohibited if nations are not already in an armed conflict and if those cyber operations intentionally cause death or physical destruction. Law professor Michael Schmitt takes a more nuanced view. His interpretation of the UN Charter is influenced by the International Court of Justice case *Nicaragua v. United States* where the court held that the United States' funding and training of the rebels constituted the use of force, despite the fact the United States did not engage militarily in the conflict. Based on this precedent, Schmitt believes several factors must be weighed to determine if a cyber attack constitutes the use of force. These factors include: the severity, measurability, and immediacy of the consequences, the directness and invasiveness of the attack, the legitimacy of the attack under domestic and international regimes, and the extent to which a state is responsible.[72] When not actively engaged in armed conflict, the military is more limited in how it may respond to a cyber attack.

Furthermore, international agreements immunize countries against aggression or intervention solely because a message transited its territory.[73] Suppose Country A launches a cyber attack on Country B, and the attack transits County C's infrastructure and occurs without Country C's knowledge. Perceivably, this doctrine would prevent Country B from retaliating against Country C. Yet, these examples of international law were developed prior to the development of modern information systems, and their relevance and interpretation in cyber warfare is still yet to be determined.

Domestic laws also influence and constrain responses to a cyber attack. As was mentioned earlier, the details of how an attack was carried out is more important for mission assurance that determining how to retaliate. If an attack was launched via a computer located in the United States, the military must defer to the Department of

---

[71] Thomas C. Wingfield, "International Law and Information Operations," in *Cyberpower and Cyberdeterrence*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 526.
[72] Michael N. Schmitt, "The Sixteenth Waldemar A. Solf Lecture in International Law," *Military Law Review* 176: 416-420.
[73] Allen, *Information Operations Planning*, 250.

Justice, who must conduct the investigation in accordance with due process requirements.[74]

The confluence of domestic law, international law, and national policy regulate the military's options for cyber defense. Together, they form the basis of rules of engagement (ROE). The ROE bounds the means available for self-defense, which will include any active defense measures.[75] The ROE may be different based the nature of the attack. Criminal activity, hostile military action, and foreign covert action against military cyberspace will yield different options available for the defender.[76] Any active defense measures that will have an impact outside of the DOD network will be subject to strict ROE and will likely require the attacker to be identified.

Summary

Cyber attacks differ from other forms of warfare, but fundamentally, cyber warfare seeks to coerce another to accede to one's desires. The major differences include compressed time, a unique geography, and a redistribution of power to a variety of actors.

Cyber warfare can produce three primary direct effects. First, it can destroy equipment. The military operates few SCADA systems, most of which control the infrastructure at permanent bases. Yet, other equipment is controlled in large part, or even exclusively, by cyber systems. These assets are difficult targets, but successful attacks could be catastrophic. The Stuxnet virus that infected Iranian nuclear facilities and the hacking of US government satellites highlight how a creative, determined attacker can circumvent static defenses. Second, attackers can cause disruption. Disruptive attacks deny the use of systems upon which the adversaries has become reliant. The effects of the attacks cannot be maintained permanently, but they do not need to be. As with other disruptive attacks, the goal is most often to cause confusion at a critical moment. Third, attackers can use cyber attacks to deceive. A highly successful attack causes the user to lose confidence in the system, thereby, losing the benefits that system provides to his operation. Each type of attack forces the victim to revert to a suboptimal operating environment.

---

[74] Levon R. Anderson, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" (Research paper, US Army War College, March 2007), 9.
[75] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 170.
[76] Wingfield, "International Law and Information Operations," 525.

Cyber defenders can mitigate some of the harmful attacks of a cyber attack and have a variety of tools to do so, along with significant constraints. They can deter. They can enact barriers to make attacks more difficult, and they can engage in an active defense. Yet, none of these approaches, even in conjunction, can eliminate the harm cyber attacks can impose. Many countermeasures, such as patching vulnerabilities, cannot keep pace with the very short time it takes to find and exploit vulnerabilities. This lag provides a window for all types of attacks.

Moreover, the diversity and unpredictability of the attack vectors and the actors makes preplanning impossible. Although there is no appreciable history of cyber warfare, the few incidents that have taken place coupled with criminal activities have shown that attackers have used creative tactics to achieve a variety of objectives. Defenders will never be able to plan for every possibility.

As will be discussed over the next two chapters, something more than defense is needed to operate in an environment that includes cyber warfare. The military must plan for the enemy to succeed in penetrating our defenses and must be in position to continue with its mission anyway. Adding a degree of resiliency is the solution.

CHAPTER 4

CONSIDERATIONS FOR RESILIENCE – CYBER CONSUMERS

Chapter 2 focused on cyberspace's benefits to the military. Chapter 3 addressed the risks posed by cyber warfare. The next two chapters examine what measures the military should take to mitigate the risk and maximize cyberspace's benefits. Chapter 4 looks at measures cyber consumers can take, while chapter 5 addresses the issues for the cyber defenders. This chapter begins with a discussion of complexity and how it relates to military operations. It continues with an examination of the human factors required to achieve resiliency. It then moves to an examination of training and exercises in degraded and denied cyber environments and the extent in which military units currently engage. Finally, the chapter explores how attacks impact the users' trust in cyber systems and what can be done to restore this trust.

Complexity of Modern Warfare

Carl von Clausewitz recognized the complexity of war without referring to formal complexity theory. Although, Clausewitz described pure war in terms of extremes, he focused not on one extreme or the other but the innumerable factors between the extremes that influence and define reality.[1] He used a variety of factors—chance, hatred, will, fog, the commander's genius, etc.—to characterize war.[2] Clausewitz compared the complexities of war to a game of cards:

> Absolute, so-called mathematical, factors never find a firm basis in military calculations. From the very start, there is an interplay of possibilities, probabilities, good luck and bad that weaves its way throughout the length and breadth of the tapestry. In the whole range of human activities, war most closely resembles a game of cards.[3]

In fact, Clausewitz's trinity resembles French mathematician Henri Poincaré's "three-body problem", the observation that given three celestial bodies small variations in any of

---

[1] See Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no. 3 (Winter 1992-1993): 66-70.
[2] Beyerchen, "Clausewitz, Nonlinearity, and Unpredictability of War," 78-79.
[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 86.

their positions, masses, or velocities will cause large variations in their predicted outcome. Poincaré's description of the "three-body problem" is credited with the discovery of chaos theory, a subset of complexity theory.[4] Alan Beyerchen claims Clausewitz echoed the effects seen in the "three-body problem" by arguing that small events in war can be disproportionally amplified.[5] Complexity theory holds that complex systems are characterized by two factors—interactions able to produce effects at the collective level that are unable to be produced at the individual level and a system that is sensitive to small perturbations.[6] Each of these is present in warfare.

It follows that if warfare is a complex system, then network-centric warfare is also complex. Ashby's Law of Requisite Variety asserts a control element of a complex system must be capable of producing at least as many responses as possible states. In the past, commanders did not have the ability to control all possible military activities and relied on subordinate commanders split into sectors to see and to respond accordingly. Today, technology allows commanders to make requisite decisions.[7] It gives them the ability to obtain adequate situational awareness and the ability to react to dynamic circumstances. Since a command and control (C2) system must have complexity requisite to the system it controls, and because cyber warfare threatens to exploit that complexity, alternate procedures are required to mitigate the risk.[8]

As discussed in chapter 2, network-centric warfare principles allow military force to be used in ways neither designed nor envisioned. Effectively, these new ways of operating increase the interactions between systems and place a greater demand on interoperability. David Fischer and Dennis Smith of Carnegie-Mellon's Software Engineering Institute said of interoperability:

> Often when problems of interoperability arise in complex systems, there is a tendency to try to gain visibility, to extend control, and to impose stronger standards. Not only are those actions ineffective in complex systems, they also increase the likelihood of certain kinds of accidents, user errors, and other failures…The frequency of normal accidents increases with the degree of coupling in systems. Coupling is increased by

[4] Daryl L. Caudle, "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers" (PhD diss., University of Phoenix, Oct 2010), 130-131.
[5] Beyerchen, "Clausewitz, Nonlinearity, and Unpredictability of War," 80.
[6] James Moffat, *Complexity Theory and Network Centric Warfare* (Washington, DC: CCRP, 2003), xi-xii.
[7] James Moffat, "Modeling Human Decision-Making," *The International C2 Journal* 1, no. 1 (2007): 33.
[8] Moffat, *Complexity Theory and Network Centric Warfare*, 46-47.

> centralized control, overly restrictive specifications, and broadly imposed interface standards. Developers of systems of systems should strive for loose coupling.[9]

Although Fischer and Smith were referring to software design, the concept holds true for C2 relationships as well. In a complex, dynamically changing environment, particularly one made more complex by the enemy's use of cyber attacks, too much centralized control and too much dependence on the other nodes is counterproductive. Fischer and Smith warn, "Centralized data and control create a single-point target for attacks…Any hierarchical structure in a complex system has the unfortunate property that every node and link in the hierarchy constitutes a single point of failure for the system of a whole."[10]

James Moffat, on the other hand, contends centralized control is needed to dampen the chaotic effects of today's modern, complex military.[11] While Moffat's contention may seem to be at odds with Fischer and Smith's warning, it is not necessarily so. Fischer and Smith warn about rigidity. Their warning seeks to avoid needless bureaucracy. Moffat's model calls for some degree of hierarchy, but the hierarchy does not have to be rigid. An organization that gives subordinates mission type orders and allows them to coordinate and collaborate with others and make decisions appropriately would fit both models.[12]

Aside from coupling and control, the notion of diversity is salient to complex systems. Rather than relying on a single type of system, commanders must devise diverse means. Otherwise, if a key vulnerability was exploited, a successful cyber attack could have terrible consequences. For a historical analogy, consider Europe's potato blight. During the Age of Discovery, the Europeans could have imported thousands of varieties of potatoes from Central and South America; instead, they bought back two. The blight that wiped out the potato crops ultimately had catastrophic consequences due to the lack

---

[9] David Fischer and Dennis B. Smith, "Emergent Issues in Interoperability," *News at SEI*, 1 March 2004, http://www.sei.cmu.edu/library/abstracts/news-at-sei/eyeonintegration20043.cfm (accessed 12 March 2012).

[10] Fischer and Smith, "Emergent Issues in Interoperability."

[11] James Moffat, *Command and Control in the Information Age* (London: The Stationary Office, 2002) in Moffat, *Complexity Theory and Network Centric Warfare*, 46-47.

[12] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 214. A mission type order is defined as "an order to a unit to perform a mission without specifying how it is to be accomplished."

of genetic diversity.[13] A complaint after Operation Iraqi Freedom (OIF) was that soldiers had to use multiple information sources. Yet, multiple systems provided a degree of diversity. This case does not suggest diversity is the ultimate goal. Too much diversity results in inefficiency.[14] The goal is to balance the needs to diversify against practical limitations to maintain efficiency and effectiveness.

Modern warfare has not eliminated the fog and friction of war. Rather, modern network-centric warfare's complexity has necessitated an even more complex C2 system. Military genius is still required to navigate the complexity, maybe more than ever.[15] The commander still must balance the need for control with the need to enable his subordinates with authority and independence. He also must balance the need to diversify with the need for efficiency and simplicity, and he must leverage the benefits of cyberspace while considering alternative procedures. Strong commanders at all levels are needed to harness the complexity.

Human and Command Factors

The notion of command must change in order to operate in a network-centric environment and to be resilient against cyber attacks. Today's commanders may find great difficulty grasping the complexity and shared risk in cyberspace. They typically lack direct expertise, and their staffs tend to have limited experience in cyber warfare.[16] Furthermore, societal and cultural differences have different interpretations of cyberspace. Due largely to a generational gap, generals and lieutenants have different viewpoints on what cyberspace even is.[17] To be successful, commanders must find ways to organize their commands and staffs, to leverage disparate skills and experiences, and to overcome gaps in knowledge.

Conventional wisdom thought network-centric warfare would flatten hierarchies. In OIF, however, the hierarchy was not flatter. The biggest difference the Army saw in OIF was a shift from staff-centric to commander-centric warfare that diffused power and

---

[13] Scott E. Page, *Diversity and Complexity* (Princeton, NJ: Princeton University Press, 2011), 8-9.
[14] Page, *Diversity and Complexity*, 2.
[15] Patrick Clowney, "Clausewitz and Network Centric Warfare: A Beautiful Message," *High Frontier* 5, no. 3 (May 2009): 38.
[16] Roy John Virden, "Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems" (Research Paper, Naval War College, 3 February 2003), 2.
[17] Caudle, "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers," 257-258.

decision making away from the headquarters staff.[18] Staffs in OIF served to monitor events and to execute the commander's wishes. They also requested less information and required fewer reports from subordinate units, since they were able to receive much of the information from networked cyber systems.[19] The Army concluded the structure of its command posts should primarily facilitate vertical and lateral communications rather than a central point of knowledge.[20] This structure, if used across the military enterprise, lessens the reliance on a single node and makes the C2 system more resilient to cyber attacks. It also reduces the tight coupling between the commander and his staff and between the subordinate commands and the headquarters staff.

A key aspect to implementing such a structure is the use of mission type orders. Mission type orders express commander's intent and require a great deal of trust in subordinates. Leaders have to be comfortable with each other, a trait that comes with familiarity and training together. Moreover, the use of mission type orders required a high degree of situational awareness over the battlefield.[21] Commanders, since they relinquish a degree of control with mission type orders, need enough confidence in the overall situation that they can issue directives without the requirement of constant intercession. In an environment with mission type orders, resilience against cyber attacks is multifaceted. Prior to mission execution, a great deal of information is required to gain the required situational awareness. During execution, the need for direct C2 is not as great, but the need to communicate and share information in order to self-synchronize operations is important. In each case, diversity plays an important role to mitigate the impact of an attack. Multiple information sources are required to build situational awareness prior to execution. Access to multiple entities and possibly multiple communication paths are required during execution.

---

[18] Dave Cammons et al., *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume I: Operations*, Center for Strategic Leadership Study (Carlisle Barracks, PA: US Army War College, 2006), 32. John B. Tisserand, III., *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume III: Network Centric Warfare Insights* (Carlisle Barracks, PA: Center for Strategic Leadership, 2006), 18.
[19] Cammons et al., *Network Centric Warfare Case Study*, 43-44.
[20] Cammons et al., *Network Centric Warfare Case Study*, 43-48.
[21] Daniel Gonzales et al. *Network Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, CA: RAND Corporation, 2005), 48.

Adaptability is another key to resiliency, and organizations and people at all levels must possess this trait. A 2010 Defense Science Board report recommended changing the DOD's culture, which focuses too heavily on "compliance, budget, and incoherent guidance." The report concedes that the military typically adapts well on the battlefield, but it contends the further away from the battlefield, the less adaptable it is.[22] Arbitrary rigidity to a process or to localized goals can have profound consequences in an interconnected, complex system. The example from chapter 2 where the Army transported fewer supplies to the front in order to maintain the speed of the main force's advance shows how support units, even those far from the fighting, have a major impact of the effectiveness of the larger mission.

The Defense Science Board advocates moving from a culture of "no" to "it can be done."[23] No longer should a unit hide behind arbitrary regulations. If a waiver to a regulation is required, it must ask for it, and the headquarters responsible for issuing the regulation must have a process to issue a waiver quickly and to modify or rescind the regulation if no longer needed.[24]

An important part of the cultural shift toward adaptability is revamping personnel practices. Military and civilian personnel in the DOD should be hired, evaluated, and promoted based on their ability to contribute to the overall mission, rather than their compliance to ancillary measures.[25] In short, the military must examine all aspects of its culture in order to become more adaptable.

Training and Exercises

A person is born with a certain amount of athletic ability, which can be enhanced through intensive training and practice. Likewise, people naturally have some degree of adaptability and resiliency ingrained in their personalities, which can be enhanced through proper training and exercises. There are several reasons why training and

---

[22] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces: Part A, Main Report* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2011), 2.
[23] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, xiv.
[24] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 151.
[25] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 122-136.

exercises enhances adaptability and, thereby, resiliency. It increases one's familiarity with their primary tasks, including teaching them the tasks' stressors and their effects. It imparts high-performance skills needed to operate in a stressful environment, and exercising successfully in a stressful environment builds confidence.[26]

As when exercising any objective, a high degree of rigor is necessary when exercising resiliency. During OIF, some units commented that their intelligence was poorer than expected, because their units had grown accustomed to a more accurate intelligence picture than could be realistically expected during exercises at the National Training Center and the Battle Command Training Program. The combination of the speed of the initial thrust into Iraq and technological limitations contributed to the units' lack of intelligence, since brigades had to have stopped for 2 hours and battalions for 8 hours in order to setup the communications capabilities to receive it.[27] Another part was the uncertainty of war and imaginative tactics of the enemy. In OIF, commanders overcame these deficiencies. In a sense, it is a positive story showing their adaptability, but it also points to a flaw in the training and exercise regime. The exercises should be creative and realistic to stress units to the limits of their abilities.

To achieve realism and rigor in cyberspace, training exercises should include more participation than just cyber units. The Air Force's exercise Black Demon uses cyber aggressor units to test its cyber defense forces, but it does not include any operational forces.[28] Exercises, such as Black Demon, are appropriate and necessary to train cyber defenders, but exercises are also needed to train non-cyber forces to continue to operate during a cyber attack. At the tactical level, some level of cyber resilience training does occur. Aircrews at the Air Force's Red Flag exercise train in various scenarios, including the loss of Global Positioning System and Link-16. The Marine Corps engages in a variety of scenarios that push decision making below the battalion level. During exercises at Fort Leavenworth and at the Joint Readiness Training Center,

[26] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 10.
[27] Cammons et al., *Network Centric Warfare Case Study*, 49-50.
[28] Andrews P. Hansen, "Cyber Flag: A Realistic Cyberspace Training Construct" (Masters' thesis, Air Force Institute of Technology, March 2008), 3. Johnnie Hernandez, "The Human Element Complicates Cybersecurity," *Defense* Systems, 2 March 2010, http://defensesystems.com/Articles/2010/03/11/Industry-Perspective-1-human-side-of-cybersecurity.aspx?Page=2 (accessed 21 March 2012).

the Army inserts cyber attacks, loss of electrical power, and the loss of intelligence, surveillance, and reconnaissance capabilities.[29]

The Defense Science Board found that training at the tactical level realistically trained forces for an environment with denial-of-service attacks; however, it also found that exercises above the tactical level lacked any significant training for the cyber threat.[30] The Air Force's Blue Flag exercise that trains airmen who operate air operations centers (AOCs) is an example of this deficiency. Despite the fact the AOC is the air component's primary C2 node, the exercise to "prepare Joint and Combined Air Component Commanders and personnel to support contingency operations worldwide" limits the veracity and intensity of the cyber attacks to keep from interfering with other training objectives.[31] Other major exercises (e.g., Ulchi Focus Lens, United Endeavor, Global Lightning) include cyber events on the mission essential synchronization lists, but the "exercises cost millions of dollars to run, and the cyber events are not allowed to have a severe impact on the exercise…How well the military could perform without cyber-enabled command and control systems may never be known until they are forced to."[32]

The major exercises that included some cyber elements focused on a binary denial of service—either the system was available or it was not.[33] Of the 11 major, operational combatant commander (COCOM) and service-level exercises in 2010, only one incorporated degraded communications. The Chairman of the Joint Chiefs of Staff recognized this discrepancy and in February 2011 ordered all major COCOM and service exercises to include realistic cyber scenarios. This order is expected to take three years to implement.[34] Full implementation of the order should test operational commands and give the military a better sense of how it would actually operate during cyber attacks.

---

[29] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 77-80.
[30] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, xii.
[31] United States Air Force, "Blue Flag," 3 March 2010, http://www.505ccw.acc.af.mil/library/factsheets/factsheet.asp?id=15317 (accessed 21 March 2012). Hansen, "Cyber Flag," 61.
[32] Jason Andress and Steve Winterfield, *Cyber Warfare: Techniques, Tactics, and Tools for Cyber Practitioners* (Waltham, MA: Syngress, 2011), 55-56.
[33] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 98-99.
[34] Department of Defense, *Director, Operational Test and Evaluation FY11 Annual Report* (Washington, DC: Office of the Director, Operational Test and Evaluation, December 2011), 285-289.

The planning costs of cyber-enabled exercises are expensive. A table-top scenario with cyber attacks takes one to two months of planning for an exercise lasting one to three days. An exercise with live cyber attacks takes 6-12 months of detailed coordination and planning for an exercise with a 2-3 month buildup period and 7-14 days of execution. Additionally, a live exercise takes money to purchase equipment and for travel costs to attend planning meetings. A live, no-notice exercise would take 12-18 months to plan for 3-month execution phase. A no-notice exercise requires senior leader involvement, clear agreements between the aggressors and operational commanders, detailed operational and technical knowledge, and significant funding.[35] To be effective, these cyber exercises should be linked to larger exercises in order to facilitate training for operating units and for cyber defenders. A no-notice cyber attack presumes a surprise attack. Very few realistic COCOM-level exercises begin with a surprise attack. Thus, the cost associated with a no-notice attack probably is not justified. However, other scenarios would benefit greatly from live cyber attacks. In these cases, the lack of realistic live cyber attacks imposes an artificiality and a false confidence on the exercises.

Of course, not all exercises must include live cyber attacks to be effective. Some adversaries have limited cyber warfare capabilities, which do not warrant significant effort on our part. However, some have more robust capabilities that could wage great harm on the US military's. MITRE analyst Jason Kick points out that there is a large difference in receiving an exercise input that says something is going awry and actually reacting to what is on the screen. "In a non-technical world, it could be compared to seeing pictures of Mt. Everest and actually climbing Mt. Everest."[36] Kick's statement especially rings true when one considers data manipulation attacks. Handing someone a card that says the data on the screen is wrong does not have the same psychological impact as not knowing for sure whether one can trust the system. Much like a flight simulator has inherent limitations in certain aspects of simulating flight, tabletop exercises have difficulties simulating deception.

Cyber ranges, that is, systems and networks that allow cyber warfare activity outside of operational systems, are part of the solution. The DOD Information Assurance

---

[35] Jason Kick, "Cyber Warfare Exercise Overview," MITRE Report, MTR 05B0000052, August 2005, 9-10.

[36] Kick, "Cyber Warfare Exercise Overview," 7.

Cyber Range is one such range. It emulates configurations found at the backbone of the NIPRNET and the SIPRNET, although it is designed with the ability to plug into service-specific ranges in order to include the services' unique capabilities. The range is capable of supporting a variety of testing, exercise, and research and development uses; however, up until this point, the range's primary use has been to train network defenders on tactical tasks. The range includes core networking equipment, firewalls, and intrusion detection tools as well traffic simulators to replicate noise normally on the network, but it lacks applications for C2, logistics, and other military functions.[37]

This limits the range's ability to integrate with major warfighting exercises. The disparity of program offices is a major hurdle for integrating these applications. For example, application X may be managed by the Army, who originally contracted with contractor A. The Air Force may oversee applications Y and Z, which were produced by contractors B and C. Application W is managed by the Defense Information Systems Agency with contractor D…and so on. The program managers have neither a vested interest nor the funding to integrate the applications into the range. Furthermore, they may not have leverage over the original contractors to modify the software or to purchase more systems, making any modifications required to integrate the applications into the range prohibitively expensive.[38]

The Chairman of the Joint Chiefs of Staff's order to develop realistic training and exercises must provide impetus to improve cyber ranges. This case is an example of where the Defense Science Board's recommendation to change the DOD's culture to encourage adaptability should be applied. Part of a program manager's evaluation should consider how well he supports the larger military mission vice meeting internal goals. This is an area where adaptability ultimately will transform into resiliency in the long term.

Trust

Military personnel trust the cyber systems will work and will provide accurate information. Yet, neither blind trust nor ardent skepticism is desirable. Rather, the level of trust an operator has in the system should be calibrated to the reliability of the

[37] Joe Minucci (DOD Cyber Range Team Lead), interview by author, 21 March 2012.
[38] Joe Minucci (DOD Cyber Range Team Lead), interview by author, 21 March 2012.

system.[39] In a cyber warfare environment, a system's reliability is based both on the system's inherent ability to operate correctly and on the likelihood the adversary will not be able to attack it successfully.

As can be seen in figure 2, there are four levels of trust of humans have in automated systems.[40]

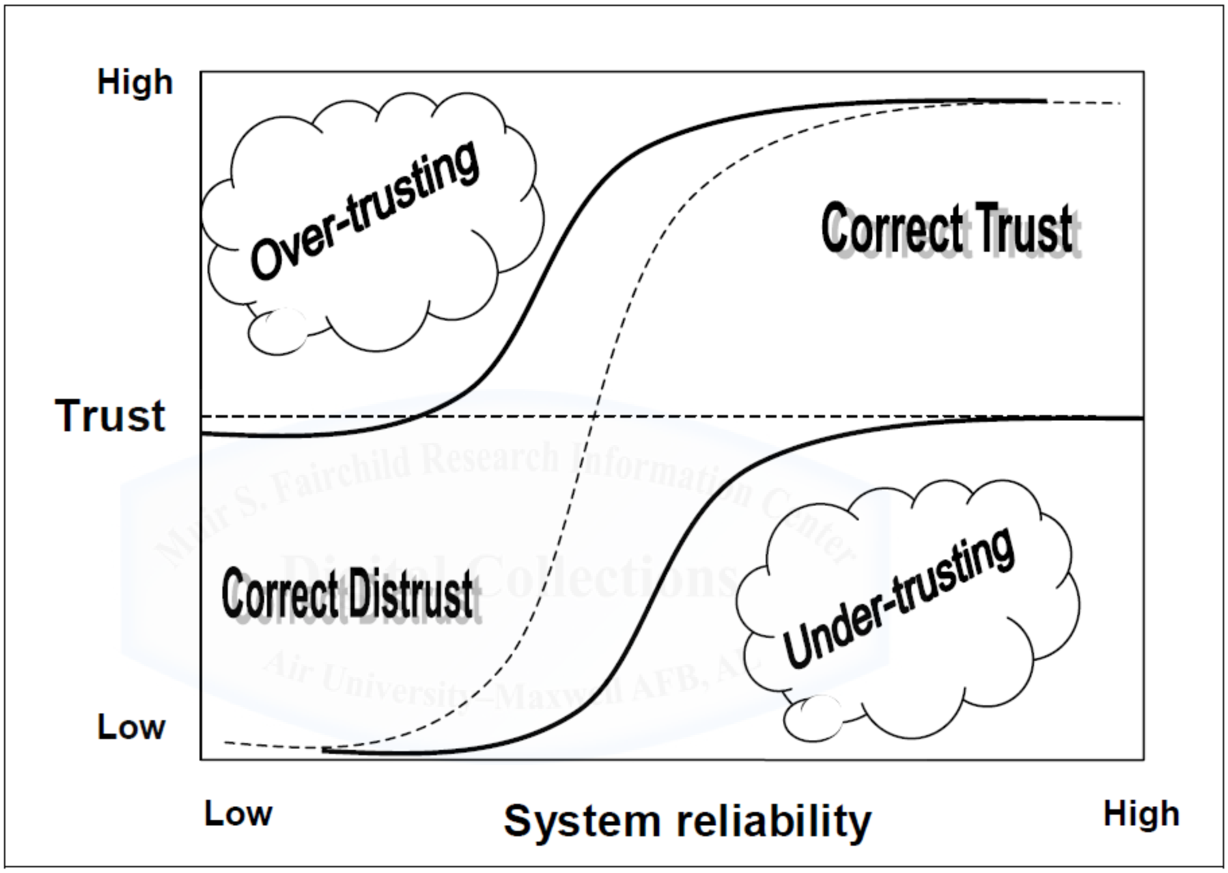

Figure 2: Trust Model and the Four Levels of Human Trust

Source: C. Kelly et al., "Guidelines for Trust in Future ATM Systems: A Literature Review," European Air Traffic Management Programme Technical Document (Brussels: European Organisation for the Safety of Air Navigation, 2003), 4.

[39] See P. Madhaven and D. A. Wiegmann, "Similarities and Difference between Human-Human and Human-Automation Trust: An Integrative Review," *Theoretical Issues in Ergonomics Study* 8, no. 4 (July-August 2007): 282. C. Kelly, "Guidelines for Trust in Future ATM Systems: A Literature Review," European Air Traffic Management Programme Technical Document (Brussels: European Organisation for the Safety of Air Navigation, 2003), 3-4. Douglas A. Wiegmann, Aaron Rich, and Hui Zhang, "Automated Diagnostic Aids: The Effects of Aid Reliability on Users' Trust and Reliance," *Theoretical Issues in Ergonomic Science* 2, no. 4 (2001): 353.

[40] C Kelly, "Guidelines for Trust in Future ATM Systems," 3-4.

If the system's reliability is poor but the user does not perceive the risk, then the user is most vulnerable to an adversary's cyber attacks, which could exploit his overreliance on the system. On the other extreme, a user can mistrust a highly reliable system. In doing so, he loses much of the value the system can provide. In the middle, a user can either correctly distrust a relatively unreliable system or correctly trust a relatively reliable one. The goal of any organization is to train its users to trust the system correctly. Since absolute trust is not practical, organizations should develop and train on alternate procedures to a degree inversely proportional to the level of reliability.

Military exercise planners, therefore, must design scenarios for cyber attacks that seek to align participants' perception of reliability to actual reliability. If exercises repeatedly deny use to a particular system that in reality is relatively reliable, over time the users will lose confidence and may under-trust the system. Likewise, exercise planners who fail to exercise attacks on more unreliable systems risk complacency taking hold.

As a non-military example, pilots overly trusted automated systems on the Airbus A320 airliner. After a January 1992 crash that was partially attributed to over-trusting the aircraft's automated systems, French officials mandated that pilots intermittently manually control the aircraft.[41] The goal of using the manual controls was not to encourage the pilots to abandon the benefits of the automated systems; rather, the policy was meant to ensure pilots maintain a certain degree of proficiency in alternate procedures, precisely because absolute reliability is impossible.

Developing exercises requires inputs from various sources. Intelligence is one source. Planners should consider potential adversaries' capabilities and doctrine. Another source is our cyber capabilities. However, the cyber attack community is generally unwilling to share its capabilities, since their use would potentially compromise their existence and thus their utility.[42] Exercise planners should not expect cutting-edge techniques from the cyber attack units. Additionally, planners should consider

---

[41] Raja Parasuraman, Robert Molloy, and Indramani L. Singh, "Performance Consequences of Automation-Induced 'Complacency'," *The International Journal of Aviation Psychology* 3, no. 1 (January 1993): 21.
[42] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare, Volume 1: Executive Summary and Annotated Brief*, SAB-TR-07-02 (Washington DC: United States Air Force, August 2007), 32.

proficiency requirements to ensure participants are familiar with standard procedures and alternate procedures.

Cyber defense personnel should play a significant roles in exercises. If one looks at a cyber system not as pieces of equipment, but something that also includes human elements, the cyber defenders are part of the system and play an important part in determining the overall system reliability. Their integration builds familiarity and gives the operators a human touch to help calibrate the reliability of the system.

None of the aforementioned aspects specifically address how to rebuild trust. Researchers have shown that the level of trust in a system falls abruptly with a fault. Trust is regained over time with lack of faults, but the restoration of trust occurs more slowly than its loss.[43] The manner trust was lost is important too. Not only must the trust be rebuilt over time, but the user must perceive that the underlying fault also has been repaired.[44]

In the context of cyber warfare, if a system were to fail in some manner at a critical moment—either by denial of service or by the user receiving false data—restoring trust would be extraordinarily difficult. While the temporal aspect of restoring trust could occur with continued fault-free operations, the user would also have to be convinced the system would not fail again in another critical moment.

Furthermore, people are more likely to distrust a machine more so than another person. While people distrust other people, they are less likely to exhibit extreme distrust. There is a stigma against distrusting another person. There is no such stigma for a machine.[45] Thus, the level of mistrust generated by cyber warfare can reach extreme levels.

Transferring system failures to a human face is essential to mitigating the extreme mistrust that invariably leads to under-trusting cyber systems and losing mission effectiveness. By dampening the degree of mistrust, the restoration of trust can occur more quickly. Cyber defense experts distributed to field units and liaison officers can help fulfill this role.

---

[43] Kelly et al., "Guidelines for Trust in Future ATM Systems," 17-18.
[44] F. David Schoorman, Roger C. Mayer, and James H. Davis, "An Integrative Model of Organizational Trust: Past, Present, and Future," *Academy of Management* Review 32, no. 2 (April 2007): 343.
[45] Madhaven and Wiegmann, "Similarities and Differences between Human-Human and Human-Automation Trust," 281.

Another concept to restore trust is through a “trust but verify” approach. Anytime one feels the need to verify, it shows a lack of trust. However, verification helps restore trust more rapidly.[46] Verifying information or occasionally reverting to a manual process is a way for operators slowly to build (or rebuild) trust.

However, the restoration of trust is not a speedy process, and the military’s goal is not to build trust blindly. Rather, its goal is to calibrate trust correctly, which includes preventing an undue loss in trust. The military’s resilience to cyber attacks hinges on its capacity to make accurate assessments of its capabilities and limitations. From a trust perspective, users will better trust a system if they understand its limitations, which incidentally helps organizations determine how much emphasis to place on alternate procedures.

Summary

For operational units, resiliency against cyber attacks comprises of control, diversity, adaptability, practice, and trust. Five major themes dominate the discussion of cyber consumers achieving resiliency. First, warfare is more complex because of cyber warfare. The C2 system must adapt in order to match the new level complexity. Redundant systems and communications paths partially fulfill this need. Command arrangements require mission type orders, and the act of command should shift to a more collegial affair. Subordinate commanders must be empowered to make decisions, in part because disruptive cyber attacks threaten isolate subordinate commanders. Subordinate commanders must have the confidence and training to operate independently—at least in the short term. To gain this trust, commanders at all levels must train together and gain familiarity.

Second, the DOD’s culture must shift to one that encourages adaptability and mission accomplishment. Both organizations and people must become more adaptable. Regulations and bureaucracy should serve an identifiable purpose and should be changed when this purpose no longer applies. Personnel practices must support the strategic mission of the military. People should be hired and rewarded based on their ability to

[46] Schoorman, Mayer, and Davis, “An Integrative Model of Organizational Trust,” 350.

meet strategic objectives rather than blind compliance to localized goals. Ultimately, this culture change must seek to foster adaptability, which will translate into resiliency.

Third, diversity of all kinds is important. From a physical perspective, operational units require multiple communications paths in order to prevent a single point of failure. Furthermore, units should have multiple information sources. Pilots do not rely on a single instrument; rather, they cross-check readings from one instrument with others. Likewise, for important functions and to prevent deception, units should use information from various sources. Hedging is a viable strategy to reduce risk, increase resiliency, and increase organizational adaptability.[47] Hedge fund investors buy a portfolio of multiple investments to limit the risk of a single failure. This concept extends to other complex systems as well.[48] Hedging in a military environment allows commanders to shift emphasis from one system or one process to another based on current conditions.

Fourth, military units of all types must train in tough, realistic conditions to prepare them to operate in a contested cyber environment. The notions of diversity, adaptability, and trust will never come to fruition unless they are tested through rigorous, realistic exercises. The exercises should seek to push the limits of the participants' ability. The exercises should educate the participants' on both the capabilities and the limitations and address competency requirements to ensure resiliency. The Chairman of the Joint Staff's directive to integrate cyber warfare into major exercises is a positive development. Its implementation must be taken seriously and not become a "check the box" requirement. Otherwise, the military risks exercising in an unrealistic environment.

Fifth, trust should be consummate with the reliability of the system. Determining this trust will largely come from exercises and the personal experiences of the users. Over-trusting the system makes users vulnerable to cyber attacks; under-trusting the system needlessly wastes mission effectiveness. Units must develop and practice alternative procedures to compensate for the residual degree of mistrust and to reduce the uncertainty associated with cyber warfare. In fact, the Air Force Scientific Advisory Board specifically recommended that all major commands in the Air Force develop

[47] Department of Defense, *Report of the Defense Science Board on Enhancing Adaptability of U.S. Military Forces*, 51.
[48] Page, *Diversity and Complexity*, 138.

tactics, techniques, and procedures for operating during a cyber attack.[49] Any measures developed must consider more than just denial-of-service attacks. The adversary's ability to alter information, which inevitably would lead to losing trust in cyber systems, must be considered. Alternate procedures—whether to address denial of service or other attacks—serve to increase diversity by eliminating reliance on a particular system or method.

[49] United States Air Force Scientific Advisory Board, *Report on Defending and Operating in a Contested Cyber Domain*, SAB-TR-08-01 (Washington DC: United States Air Force, August 2008), vii.

CHAPTER 5

CONSIDERATIONS FOR RESILIENCE – CYBER DEFENDERS

While alternate operating procedures have their place, the application of military force is suboptimal when using alternate operating procedures. Recovery from cyber attacks limits the damage the enemy can impose and ensures the military returns to its fullest operating capability. This chapter explores what cyber defenders can and should do to limit the damage from a cyber attack. It begins with a discussion on the basic roles of information assurance and cyber defense. It follows with an examination of the current structure of cyber defense and how this structure contributes to resilience. The chapter then looks at the synchronization of cyber defense operations with other military operations. How do cyber defenders plan to support operations prior to execution? What are the salient aspects of identifying an ongoing cyber attack? This chapter also describes the actions defenders must take to stop further damage and return to a normal state of operations.

Information Assurance's Role

The protective measures imposed by information assurance play an important role in obtaining resiliency. As discussed in chapter 3, information assurance is the passive defense of cyberspace. Just as fortifications in land warfare can slow an attack and limit its intensity, information assurance measures serve as a barrier that screens potential cyber attacks. Thus, cyber defenders have fewer active threats with which to concern themselves, which allows them to devote more effort to recovery and restoration. The Government Communications Headquarters, the United Kingdom's equivalent to the United States' National Security Agency, estimates that 80% of the government's cyber vulnerabilities can be closed with existing information assurance and personnel security measures.[1] The implementation of the DOD's Common Access Card (CAC) is a good

[1] U.K. House of Commons Library, *Cyber Security: A New National Programme*, by Emma Downing, Standard Note SN/SC/5832 (London: Parliament, 23 June 2001), 6.

example of this principle. Once the CAC was implemented, the number of intrusions into DOD systems fell by 50 percent.[2]

Software

Information assurance covers a broad scope of security measures, including software development. One proactive information assurance technique is the inclusion of deceptive traps in software. Tools, such as Deception Toolkit, allow developers to program deceptive features into the code. Essentially, camouflage and concealment features are inserted into the computer code.[3] Potential attackers are more likely to muddle through the deceptive aspects of the code. This may delay the attackers in finding a vulnerability they can exploit. In a best case scenario, the attackers may be fooled to attempt to exploit a vulnerability that does not actually exist, thus giving defenders a better opportunity to discern the intent of the attacker. This technique is not applicable to all software, but it is a viable option for custom software—software that tends to have the most direct impact on combat operations.

Security Regime

The security regime specified by the information assurance process complements software measures. A strong security regime prevents many attacks from occurring in the first place. However, a one-size-fits-all approach is impossible. At the DOD level, the system has too many variables to impose overly broad, overly rigid security measures. For example, the implementation of the CAC may have stopped many attacks, but requiring full use of CAC authentication for every network transaction is impractical. Contractors, vendors, coalition partners, and legacy systems all use military networks, and requiring all of them to obtain CACs would unduly impose delays in the system.[4] At the lower levels, units have a better picture of their operational needs, but commanders and support personnel lack the skills necessary to develop a robust security regime. As such, any security regime will always be incomplete. The military must not overpay for any security regime, which will be rigid, incomplete, or both.

---

[2] James R. Langevin et al., *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008), 62.

[3] Fred Cohen, "A Note on the Role of Deception in Information Protection," Fred Cohen and Associates, 1998, http://all.net/journal/deception/deception.html (accessed on 7 April 2012).

[4] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare, Volume 2: Final Report*, SAB-TR-07-02 (Washington DC: United States Air Force, August 2007), 35.

Skilled, creative attackers can breach cyber fortifications. The White House's *International Strategy for Cyberspace* acknowledges the weaknesses of a security approach and specifically states that the United States will not pursue a national filter or a national firewall.[5] The expense of building such a grandiose project coupled with the realistic assumption that many types of attacks will bypass it does not justify the potential benefit. Cyber attackers have demonstrated the ability to be dynamic and creative. Passive defenses are important, but they cannot stop a thinking enemy.

The inability for defenders to react is apparent in the software patch and deployment process—a process that traditionally has been associated with information assurance. Once a vulnerability is publically discovered in commercial software, hackers create an exploit tool in an average of one to five days. In contrast, software developers take an average of 22-122 days to create a patch. Once a patch is developed, administrators take on the order of weeks or months to deploy it.[6] In the interim, attackers have a window to attack at little cost.

The reliance on patching is more daunting when one considers supply chain attacks. Hardware and software production is a global industry. With all of the permutations of where and how hardware and software are produced, the information assurance process, no matter how strict and how robust, cannot guarantee the supply chain is secure.[7] At best, the information assurance process can identify the nations that produce the hardware and software. The process cannot guarantee the products' code is free of vulnerabilities left by a developer.

Cyber Defense's Role

The intent of highlighting information assurance's deficiencies is not to invalidate its utility. Rather, the point is to illustrate that additional, more flexible measures are

[5] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, 5.
[6] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare, Volume 1: Executive Summary and Annotated Brief*, SAB-TR-07-02 (Washington DC: United States Air Force, August 2007), 12-13. The length of time to create a patch for custom software is longer and may be significantly longer depending on the circumstances.
[7] Paul Rosenzweig, "National Security Issues in Cyberspace," Post workshop report of the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum, Annapolis, MD, September 2009, 1.

needed to assure the military can continue to operate in contested cyberspace. Active defense measures are necessary to counter a dynamic enemy who launches a cyber attack.

Computer security expert Patrick Allen proposes five principles for cyber defense. First, defenders must have a variety of contingency plans for different enemies, different timeframes, and different sets of responses. Second, defensive measures must do less harm than good. Third, defenders must have sufficient flexibility in their response options. Related this principle is his fourth principle—defenders must plan on how to handle surprises. Finally, defenders must have flexibility in the visibility of their defenses. In other words, cyber defense should have a varying degree of visibility to a potential attacker.[8] Take security for a major event, for instance. Uniformed security agents are visible to show presence, while undercover agents blend into the crowd to provide surprise.

Allen's cyber defense principles build on the foundation of information assurance. They add flexibility to an otherwise inflexible passive defense structure. A primary role for the cyber defender is to bind these principles to military operations. Cyber defense contingency plans must be intertwined with operational plans. Response measures to cyber attacks must incorporate the costs and benefits to the operational forces, and operational forces and cyber defenders must share a degree of understanding of each other's environment. The military's cyber defenders do not defend the network for its own sake. Rather, they impart their skills to obtain a greater military objective.

Current Organization

The structure of any military organization plays a major role in how command and control is accomplished and how tasks are prioritized. The current structure of cyber defense is important to understanding how cyber defenders and operational units interact. A major prerequisite to understand the organizational structure of cyber defense requires understanding the organization of the networks.

Network Organization

A network consists of multiple machines containing data as well as the media that links them together. Even seemingly stand-alone machines are often networked. For

---

[8] Patrick D. Allen, *Information Operations Planning* (Norwood, MA: Artech House, 2007), 147-153.

example, a flight-planning computer for a fighter jet transfers information via hardware carried between the terminal and the jet. Updates to the terminal are handled by a centralized program office and distributed to each flight planning computer.[9] This simple network transcends across multiple organizations—the fighter units and the program office at a minimum.

For more complex networks, servers provide data to various devices in the network. A network could consolidate information and services, or it could distribute services across many machines. Servers could be distributed in a hierarchical architecture or from a centralized location. The move towards data centers and cloud computing is prevalent throughout both the military and commercial industry.

Data centers provide a large number of common services across the military. The DOD operates 772 data centers, including 14 Defense Enterprise Computer Centers run by the Defense Information Systems Agency (DISA). These data centers host a variety of services, including anything from e-mail to command and control (C2) systems to logistics data to intelligence databases.[10] Organizationally, the primary responsibility for defense rests with the operator of the data center (e.g., DISA, if hosted at a Defense Enterprise Computing Center). A much lesser degree of responsibility rests with the authorized users of the service.

Cloud computing is the next leap forward from traditional data centers. Cloud computing is a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources," which essentially works like a utility grid that dynamically allocates resources from multiple sources.[11] The US Chief Information Officer has dictated a "cloud first" policy where all government entities, including the military, should seek to utilize a cloud architecture if possible.[12] The *Department of Defense Strategy for Operating in Cyberspace* embraces cloud computing

[9] 309 Software Maintenance Group, "Mission Planning," http://www.309smxg.hill.af.mil/solutions/mission_planning.html (accessed 1 May 2012).
[10] Greg Slabodkin, "DISA Outlines Major Network and Enterprise Initiatives," *Defense Systems*, 1 April 2011, http://defensesystems.com/Articles/2011/03/29/Cover-Story-DISA-charts-cloud-strategy.aspx (accessed 7 April 2012).
[11] Department of Commerce, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Washington, DC: National Institute of Standards and Technology, September 2011), 2.
[12] Vivek Kundra, *Federal Cloud Computing Strategy* (Washington, DC: US Chief Information Officer, 8 February 2011), 2, 22-23.

as a way to foster resiliency.[13] Cloud computing disperses critical information over multiple geographic locations. The loss of a single component is generally not a problem. Although cloud computing mitigates machine-level vulnerabilities, it is extremely vulnerable if the cloud's management apparatus is compromised.[14] Much like the European potato analogy from chapter 4, the consequences of a successful attack on the cloud's management apparatus would be catastrophic. The tide is moving toward cloud computing, which offers opportunities and challenges. The military cannot put all of its eggs in the same cloud. It must allow for the possibility that an entire cloud may be lost and plan accordingly.

The linkages that link the information sources represent the other major aspect of a network. A variety of media—fiber-optic-cable, terrestrial radio frequency links, satellites, etc.—connect devices on a network. For Internet Protocol (IP) networks—such as NIPRNET, SIPRNET, and JWICS—routers and switches direct data to its proper destination. Organizationally, the owner of the network's equipment is responsible for its defense.

IP networks, among others, support dynamic routing and may route traffic differently based on non-availability or congestion of a link. Thus, information may transverse different networks at different times. In many ways, lower-level defenders do not defend the information; they defend the links. However, these defenders' actions can have significant impact on the information that flows across their networks.

Organization of Cyber Defenses

The passive defense (information assurance) and active defense of military cyberspace is organizationally split. At the top of level of a network, the head of the organization responsible for it appoints a Designated Approval Authority (DAA) to set security policies and offset risks.[15] The DAA dictates procedures for networks, hardware, and software to connect to or reside on a network. Each of these connections requires a security assessment. The DAA also dictates the required security infrastructure, which

---

[13] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Office of the Secretary of Defense, July 2011), 7. In fact, the Army recently moved all of its unclassified and secret e-mail to a cloud architecture run by the DISA hosted across nine physical locations. See Slabodkin, "DISA Outlines Major Network and Enterprise Initiatives."

[14] Rosenzweig, "National Security Issues in Cyberspace," 25.

[15] Department of Defense Directive (DODD) 8500.01E, *Information Assurance (IA)*, 24 October 2002, 11

includes firewalls, intrusion detection systems, and other devices. For a practical example, the Defense Information Systems Network (DISN), which includes NIPRNET, SIPRNET, and the Defense Switched Network (DSN) telephones, has a committee of four DAAs.[16] This committee sets policy on how other networks, hardware, and software can connect to the DISN. The DISN includes firewalls and other security systems throughout the network. If an Air Force network wanted to connect to the DISN—such as the Air Force Satellite Control Network— it would have to conform to the DISN DAAs' security policies. Subject to the DISN DAAs' specific requirements, the DAA for the Air Force network would then approve software and hardware for the Air Force Satellite Control Network and would prescribe specific security measures. In large part, those who own the physical equipment impose the information assurance measures.

Whereas information assurance falls under the purview of the communications service provider (i.e., J-6, A-6, S-6, etc.), cyber defense is a component of information operations and falls under operations (i.e., J-3, A-3, S-3, etc.).[17] US Cyber Command (USCYBERCOM) has responsibility to defend the DISN and may task DISN operators and service components. Each of the services has cyber defense units for their portions of the DISN. Below the service level, few personnel are dedicated to cyber defense tasks, and non-DISN networks have various models of how they defend their networks. Some non-DISN networks have little more than system administrators who occasionally check the logs.

Pre-Attack Planning

The military plans for a variety of contingencies across the spectrum of conflict. It is a process in which cyber defenders must participate. Cyber defenders must have knowledge of how the Joint Force Commander (JFC) will use cyberspace in the context of a larger operational scheme to ensure appropriate measures are in place to assure resiliency.

Cyber defense specialists are a limited resource. They rely on network and system administrators to augment their ability to response to attacks. The administrators are in a

[16] DODD 8500.01E, *Information* Assurance, 16. The Defense Information Systems Network DAAs consist of the Director, Defense Information Systems Agency; Director, Defense Intelligence Agency; Director, National Security Agency; and Director, Joint Staff.
[17] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, II-4 – II-6, IV-3 – IV-6.

first-hand position to determine when the system does not look right and when it is operating abnormally. Network and systems administrators are paid to be technicians not to plan military operations. However, if sensitized to a potential threat or to a potential type of attack, the administrators can serve as lookouts and deployed sensors.

Calibrating cyber operators and cyber defenders to the JFC's priorities reduces the time needed to react to problems. For example, operators in the United States fly the Predator Unmanned Aerial Vehicle (UAV) via communications links.[18] If the UAV is critical to the JFC, and if a major node or link goes down for any reason, then the network administrator may have to reroute traffic to available bandwidth.[19] Prior knowledge of the mission would enable the network administrator to understand what links and nodes are critical and what services to prioritize. Should the outage have been caused by enemy action rather than system failure, cyber defenders could take steps to mitigate the threat.

Not only must cyber defenders have knowledge the JFC's operational plan, they must also have knowledge of the enemy. Although resiliency, in part, depends on the ability to weather the unknown, resiliency also requires being able to anticipate threats and being prepared to counter them. As part of the planning process, cyber defenders, in conjunction with the JFC's other staff functions, should conduct cyber intelligence preparation of the battlefield (IPB). The Army defines IPB as "a systematic, continuous process of analyzing the threat and environment."[20] The result of IPB should:

- define the battlefield environment;
- describe the battlefield's effects;
- evaluate the threat;
- determine threat courses of action.[21]

In a cyber environment, the IPB process would consider: the enemy and friendly uses of cyberspace, the types of hardware and software used, the skill of system administrators

[18] United States Air Force, "Predator Combat Air Patrols Double in 1 Year," 6 May 2008, http://www.af.mil/news/story.asp?id=123097395 (accessed 23 January 2012).
[19] In many cases, the system will dynamically reroute the traffic. However, an outage may restrict the amount of available. In this case, the network administrator would have to determine how traffic would be routed.
[20] Field Manual (FM) 34-130, *Intelligence Preparation of the* Battlefield, 8 July 1994, 1-1.
[21] FM 34-130, *Intelligence Preparation of the Battlefield*, 1-1.

and cyber warfare personnel, the cyber vulnerabilities and dependencies for each side, known offensive and defensive tactics, the possible use of third parties, and the enemy's most likely and most dangerous courses of action in cyberspace.[22] The IPB process will guide information assurance measures prior to actual conflict, including how the security architecture will be built. It will also inform cyber defenders on what to expect and will help them develop tactics to counter the threat. General Kevin Chilton, then commander of US Strategic Command, spoke of the importance of marrying the intelligence, information assurance, and cyber defense processes, "I believe that, ultimately, we have to be even faster than network speed if we're going to defend this network appropriately. How do we do that? I'm not suggesting that we defy the laws of physics. We do it by focused, high-tech, all-source intelligence that tries to anticipate threats before they even arrive. We have to be able to anticipate attacks and intrusions and, when we can, preempt those threats before they arrive at our bases, posts, camps, or stations—or at the laptops on our desks."[23]

Part of the IPB process must include a vulnerability assessment on friendly systems by a cyber red team. As already discussed, proper security measures can eliminate many, or even most, of the military's cyber vulnerabilities. By closing eliminating vulnerabilities, the military is denying the enemy potential pre-planned avenues of attack. If the enemy were to attempt to exploit a recently closed vulnerability, defenders would have some indication of an attack, providing valuable insight into the enemy's intent, attack platforms, and tactics.

Furthermore, the planning process and IPB may drive the redeployment of defensive resources. A honeypot is a dummy system or network designed to deceive attackers into thinking they are attacking an actual network.[24] Depending on the situation, it can be used to divert attention away from a legitimate target and serve as a way to collect intelligence on the enemy's tactics. However, there is a risk in deploying honeypots too late. If the enemy has already mapped the network, the introduction of a

---

[22] Steven P. Winterfield, "Cyber IPB" (GSEC paper submission, December 2001), http://www.giac.org/paper/gsec/1752/cyber-ipb/103147 (accessed 15 April 2012).
[23] Kevin P. Chilton, "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal* 23, no. 3 (Fall 2009), http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/chilton.html (accessed 15 April 2012).
[24] Allen, *Information Operations Planning*, 45.

honeypot may signal the importance of a system or give the enemy an opportunity to engage in counter-deception.[25] Yet, if friendly forces require a great deal of build up or substantially change their networks, the inclusion of a honeypot may help provide valuable intelligence and even early warning.

Pre-attack planning requires the integration of information assurance and cyber defense elements with the operations and intelligence elements of the operational planning process. Doing so increases situational awareness, which decreases the lag time to react to a potential problem. Prior planning also optimizes the system's structure to meet a tailored threat.

Detecting an Attack

Resilience depends in part on detecting enemy actions. The need to identify an attack may not be a requirement for resilience in every case. For example, a series of inconsequential attacks or unsuccessful attacks do not impact the military's ability to execute its mission. However, in many cases, the need to know one is being attacked is vital to mission assurance in the long run.

Dr. Kamal Jabbour, the Senior Scientist for Information Assurance at the Air Force Research Laboratory, contends there are three primary aspects of cyber situational awareness. First, the cyber situational awareness process must perceive an attack. Second, the process should add to the comprehension of the situation. It must be able to include events in the proper context. Third, the system should give the ability to project into the future.[26] Planning and cyber IPB largely satisfies Jabbour's latter two aspects. Jabbour's first contention requires more discussion.

In the traditional domains, perceiving an attack is fairly self-evident. In cyberspace, knowing whether or not an attack took place may not be so clear. When a system goes down, it may not be obvious whether it was from system failure or an attack. System administrators may even ignore signs of an attack in attempt to restore service. The system administrator's effort enhance resiliency in one regard, since administrators work quickly to restore the system to full mission capability. In another regard, if service

---

[25] Allen, *Information Operations Planning*, 45, 152.

[26] Kamal Jabbour, "The Science and Technology of Cyber Operations," *High Frontier* 5, no. 3 (May 2009): 11.

was lost due to an attack, restoral actions cause the military to lose valuable information on the enemy's capabilities. As will be discussed later, system administrators must balance the quest for knowledge on why a system failed against efficiency.

If the enemy uses a cyber attack intended to deceive, the victim may not even know he is under attack. In general, humans are not good at detecting deception. Some studies suggest humans can detect deception only about 50 percent of the time.[27] To compensate, cyber defenders must employ more sophisticated means to aid in detecting deception.

Another major aspect of cyber situational awareness is the integration of counterintelligence with cyber defense. In the course of either vulnerability scans, cyber defense techniques, or intelligence, defenders may learn of enemy intrusions of friendly cyberspace. At times, it is better to observe the enemy rather than root out the intruder. Observing the intruders allows defenders to learn about the enemy's intent and tactics.[28] Ideally, this counter-surveillance would occur in context of a honeypot or in a non-critical network, such as a public web server. One can compare this concept to law enforcement agencies foregoing arrests in an organized crime ring so they can observe activity that leads them to bigger criminals. The article "When Not to Pull the Plug" likens counter-surveillance in cyberspace to the Army's doctrine on area defense. Specifically, it quotes Army Field Manual 3-90, "As the enemy's attack begins, the defending unit's first concerns are identify committed enemy units' positions and capabilities, determine the enemy units' intent and direction of attack, and gain time to react."[29] As in the physical world, knowing the enemy's position, intent, and tactics helps decrease reaction time, which conversely, decreases the impact and duration of cyber attacks. Unlike the physical world, the enemy can attack in cyberspace instantaneously. Defenders must deny potential attacks before they significantly harm the US military's mission.

Of course, cyber defenders normally must ascertain the identity of an intruder to engage in counter-surveillance. Due to legal and political considerations, the identity of

---

[27] Judee K. Burgoon and Jay F. Nunamaker, Jr., eds., "Toward Computer-Aided Support for the Detection of Deception," *Group Decision and Negotiation* 13 (2004): 1.
[28] Scott Knight and Sylvain LeBlanc, "When Not to Pull the Plug: The Need for Counter-Surveillance," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Fairfax, VA: IOS Press, 2009), 226.
[29] Quoted in Knight and LeBlanc, "When Not to Pull the Plug," 226.

an unknown attacker may be pertinent to defense and recovery. Is the attacker the hostile party? Is it a proxy for the hostile party? Is it a sympathizer? Is the attacker actually another party seeking to collect intelligence and not to attack? Particularly at the more aggressive end of the active defense spectrum, the identity of the attacker may determine if counteroffensive action is legal.

At the same time as cyber defenders are attributing the source and the nature of the attack, they must also determine the operational impact of the attack. Damage assessment is critical function of command and control and is an important factor in how commanders allocate resources.[30] Cyber defense assets are limited. In an environment where they must defend against multiple threats, commanders will have to prioritize the defenders' efforts. Those attacks with greater operational impact demand greater attention.

The current cyber defense paradigm does not offer a robust method to assess operational impact. USCYBERCOM is in the process of building cyber support elements at each of the geographic combatant commands. These elements will serve as liaisons and will provide technical advice. As of March 2012, only one element is in place, and another is partially operational.[31] Theoretically, these elements could sit in the Joint Operations Center and report to USCYBERCOM on mission impact.[32] USCYBERCOM could then task subordinate units, including DISA organizations that operate defense-wide data centers and "cloud" networks, to take measures to stop the attack and to restore service. Alternatively, units experiencing operational impact could go through service channels. However, unless dual reporting is enforced, service channels cut out the JFC. Even if the JFC was informed, he would not have the authority to prioritize or direct the services' cyber defense capabilities.

The JFC is responsible for the execution of the mission. The JFC should create an element in the Joint Operations Center to assess and relay the operational impact of a cyber attack and to direct response actions to these attacks from the cyber defense

[30] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics regarding U.S. Acquisition of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 130.
[31] Zachary Fryer-Biggs, "US Military Goes on the Cyber Offensive," *Federal Times*, 26 March 2012, http://www.federaltimes.com/article/20120326/DEPARTMENTS01/203260301/ (accessed 21 April 2012).
[32] USCYBERCOM currently only defends the NIPRNET and SIPRNET. For attacks on other networks, the Joint Force Commanders would have to report through separate channels.

capabilities the JFC controls.[33] The element may consist of an individual or consist of a team. The element may have other responsibilities, but it must have expertise in cyber warfare and must be in a position to understand the commander's broad scheme of maneuver and how cyberspace contributes to it. Since cyber attacks and their effects can occur without warning, this element must be integrated into the Joint Operations Center and not merely be part of the staff structure. The Joint Operations Center is the eyes and ears of the commander. It is often his mouth as well. The Joint Operation Center's involvement is necessary to communicate mission impact and to task cyber defense entities appropriately to restore service.

Cyber defenders also have the responsibility to report their findings horizontally across the organization. At present, the lack of coordination and collaboration hurts the ability to engage in active defense.[34] The details of an attack will help cyber defenders at all levels prevent copycat attacks and will decrease the effectiveness of the enemy's weapon. For data manipulation attacks, knowing the details of the attack and preventing it—or at least recognizing it as early as possible—is far better than relying on users to detect incorrect data on their own. Furthermore, the users should not lose as much trust in the system if a cyber defender informs them of a problem vice if the user is forced to discover it.

Aside from denying similar attacks, the actual use of cyber attacks and the types of cyber attacks may be critical indicators of future enemy activity. Prior to a decisive point in the conflict, it is in the enemy's best interest to avoid attacks on key systems.[35] The enemy may have more to gain from collecting intelligence on the system rather than attacking it. A denial attack suffers from the inability of the attack's effects to persist. The enemy knows that the defender will restore the capability. Hence, the time immediately after a disruptive cyber attack is dangerous, as it may indicate the enemy is trying to throw its opponent off guard. As this case shows, cyber defenders must have a proven mechanism to report hostile activity to operational commanders. Another

---

[33] Joint Publication (JP) 3-33, *Joint Task Force Headquarters*, 16 February 2007, VII-3 – VII-6, describes the doctrinal role of a joint operations center.
[34] Daryl L. Caudle, "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers" (PhD diss., University of Phoenix, Oct 2010), 265.
[35] Department of the Air Force, *Report on Defending and Operating in a Contested Cyber Domain*, SAB-TR-08-01 (Washington, DC: United States Air Force Scientific Advisory Board, 31 August 2008), 25.

dangerous time (and one that should also be reported) is immediately after applying cyber defense measures. Once the military starts applying cyber defense measures, if the enemy has a tool to exploit a vulnerability that is in the process of being closed, he is in a "use it or lose it" situation. In this situation, cyber defense and operational entities must understand they may come under cyber attack simply because the enemy may calculate he has nothing to lose by not attacking at this time or, more accurately, nothing to gain by waiting.

Defense-in-Depth

Defense-in-depth is critical to maintaining resiliency against cyber attacks. No military base would rely on a fence with guards only at an entry point for its entire defense. In reality, bases have roving patrol—both inside and sometimes outside of the fence. Base personnel build and, if necessary, man defensive fighting positions at vital points. Air defense units may provide protection from airborne threats. This list could go on, but the point is that a military base layers its defenses and so do defenses in cyberspace.

Cyber defenders face multiple adversaries using multiple attack vectors and defend diverse capabilities that support a variety of operational missions. Defenses at various levels are appropriate.[36] At the lowest level, the defenders are most likely to know the networks and discern abnormalities. At the highest level, the defenders screen potential hostile actors. The different layers confuse the enemy by giving him multiple defense paradigms to have to defeat and increase the chances defenders will detect hostile activity. Defense-in-depth's natural diversity helps increase resiliency in cyberspace.

Active Defense Measures and Maneuverability

Defensive structures alone cannot guarantee resiliency. Active defense measures and maneuverability are essential to stemming an attack. Networks can become static. In doing so, they cede the initiative and, therefore, the advantage to the attacker. In its military context, maneuver is defined as the "employment of forces in the operational area through movement in combination with fires *to achieve a position of advantage with*

---

[36] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, Franklin P. Kramer, Stuart H. Starr, and Larry K. Wentz, eds. (Dulles, VA: Penguin Books, 2009), 310.

respect to the enemy."[37] In the case of cyber maneuverability, the defender moves in virtual space in order to buy time to react to the enemy.

Cyber defenders maneuver is various ways. They can dynamically create honeypots in unused areas of the network, change configurations (the cyber equivalent of war reserve frequencies), update patches, and move elements of the network to new addresses.[38] In short, cyber defenders can take steps to deceive the attacker and to frustrate his efforts. Deception is a key component of cyber maneuverability. Deception is based on the art of simultaneously hiding and showing things at the same time.[39] The attacker will see information, but the defender may have non-standard file names, spoofed IP addresses, simulated effects making attacker think he was successful, additional network traffic to induce noise, or placement of a valuable system in a large network to blend in with similar systems.[40]

An alternative method of maneuver is to move to an entirely different architecture on a temporary basis. For instance, civilian servers could host information and applications for a short time until military servers can be restored.[41]

The Estonian government's response to the 2007 cyber attacks shows how maneuver may apply in the future. Attacked from multiple sources, the Estonian government sacrificed its presidential website. It deemed this site non-critical and chose to focus its limited cyber defense capability on more critical systems. Meanwhile, the hackers continued to focus on the presidential site.[42] With the assistance of the United States, critical services moved onto commercial servers, which had advantages in

---

[37] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 200 [Emphasis added].
[38] Keith Repik, "Defeating Adversary Network Intelligence Effort with Active Cyber Defense Techniques," (Master's thesis, Air Force Institute of Technology, June 2008), 10-11. Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics regarding U.S. Acquisition of Cyberattack Capabilities*, 120-121.
[39] Jim Yuill, Dorothy Denning, and Fred Feer, "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques," *Journal of Information Warfare* 5, no 3. (November 2006): 28.
[40] Kheng Lee Gregory Tan, "Confronting Cyberterrorism with Cyber Deception," (Master's thesis, Naval Postgraduate School, December 2003), 42-46. Yuill, Denning, and Feer, "Using Deception to Hide Things from Hackers," 32-33.
[41] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare, Volume 2*, 57.
[42] Mike Collier, "Estonia: Cyber Superpower," *Business Week*, 17 Dec 2007, http://www.businessweek.com/globalbiz/content/dec2007/gb20071217_535635.htm (accessed 16 March 2012).

bandwidth and the ability to filter attacks.[43] In the end, the cyber attacks against one of the most wired countries on earth equated to little more than an inconvenience.[44]

Maneuverability bought the Estonians time and undoubtedly contributed to their resilience, but maneuver's purpose is to gain an advantage. A more aggressive response to a cyber attack may help achieve resiliency in certain circumstances. Computer network defense response actions refer to real-time actions to contain attacks and may include offensive actions.[45] An example of an offensive action is a counterattack against a botnet controller to stop a distributed denial-of-service attack.[46] Legal and political restrictions limit the use of the many offensive techniques due to the difficulty in obtaining reliable attribution of the source in a timely manner.[47] However, a cyber counterattack is a possibility given the right context. If the operational impact is high enough and the mission important enough, the rules of engagement and collateral damage considerations will become more lenient. Cyber defenders should consider offensive action as part of a toolkit to stop attacks and further the larger military mission.

Restoral of Services

Ultimately, the ability to restore services in a timely manner is a primary factor in rendering the military resilient against cyber attacks. The goal of a cyber attack against the military is to degrade its capability in order to gain an advantage. Cyber defenders must stem this attack and, in conjunction with cyber service providers, restore military power by providing the full use of cyberspace.

In general, attackers either attack the information or the links in the system. If a link or set of links is denied, cyber defenders must find ways to shift the load. As discussed in chapter 2, the military relies heavily on satellites to provide information to combat units. Overreliance on space-based systems presents a particularly daunting challenge.

---

[43] Kugler, "Deterrence of Cyber Attacks," 313.
[44] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics regarding U.S. Acquisition of Cyberattack Capabilities*, 172.
[45] Jabbour, "The Science and Technology of Cyber Operations," 15.
[46] Felix Leder, Tillman Werner, and Peter Martini, "Proactive Botnet Countermeasures: An Offensive Approach," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Fairfax, VA: IOS Press, 2009), 214-216.
[47] Jabbour, "The Science and Technology of Cyber Operations," 15.

Satellites currently in orbit suffer from saturation.[48] The military already relies heavily on commercial providers for communications, imagery, and launch capabilities. At the height of Operations Enduring Freedom and Iraqi Freedom, the military relied on commercial satellites for 80 percent of its satellite communications, including all of its blue force tracking dissemination and to operate the Air Force's UAV fleet.[49] The estimated bandwidth the military will require in a future conflicts ranges from two to nine times more than that needed in the Iraq and Afghanistan conflicts.[50] Even for the low estimate, the future suggests a saturated satellite network with little room to absorb damage from enemy operations. The military has not shown the propensity to replenish its space-based capabilities. The commercial space market cannot handle the demand to diversify or to replenish satellites lost during conflict. Market forces also preclude the inclusion of certain types of military missions on commercial platforms. In essence, what is currently in orbit will be what is available during the entirety of a conflict, even if the satellites receive damage. Since the US commercial market cannot handle a surge, in times of conflict, the US may have to fall back on the commercial capabilities of friendly nations for surge capacity.[51]

Due in part to the constraints of satellites, the military must identify bandwidth chokepoints and mitigate them.[52] The Army concluded after Operation Iraqi Freedom that "bandwidth must be treated as a high-demand, low-density 'class of supply' requiring command attention."[53] This statement is not a pronouncement of how to engineer the

[48] Sean Gallagher, "Satcom at a Crossroads," http://defensesystems.com/articles/2009/06/10/tech-focus-satellite-communications.aspx (accessed 15 January 2012).
[49] John Edwards, "Commercial Sat Market Stirs", *Aviation Week and Space Technology* 162, no. 3 (17 January 2005): 147-150. Tisserand, *Network Centric Warfare Case Study*, *Vol. III*, D-2 – D-4. The author's is familiar with architectures of the Predator and Global Hawk systems based on his experiences while deployed to USCENTCOM.
[50] Greg Berlocher, "Military Continues to Influence Commercial Operators," *Satellite Today*, 1 September 2008, http://www.satellitetoday.com/military/netwarfare/Military-Continues-To-Influence-Commercial-Operators_24295_p2.html (accessed 15 January 2012).
[51] This may not be an easy proposition. Nations and/or companies may wish to avoid US military traffic in order to maintain a perception of neutrality. Even companies in allied nations may refuse military traffic to avoid the possibility of becoming the next space casualties. While the US may be able to persuade, coerce, of compel American service providers, it would likely have significantly less sway for foreign providers. Using foreign companies as surge capacity is the best of bad options.
[52] Gregory J. Rattray, "An Environmental Approach to Cyberpower," *in Cyberpower and National Security*, 269.
[53] Dave Cammons et al., *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume I:*

communications architecture; rather, the Army's assertion is based on the need to determine who gets limited resources, particularly if hostile actions limit bandwidth availability.

Part of the bandwidth problem can be solved by using means not normally employed in today's military. Expanded use of "legacy" technologies—such as high frequency and troposcatter radio—mitigate the impact. These technologies are inferior many ways, but if used as emergency capacity, they provide an over-the-horizon capability that is re-locatable and reconfigurable. These technologies provide either a bridge capability or a backup capability to space-based systems.

New capabilities can also mitigate bandwidth concerns, particularly those resulting from the denial of space-based assets. The Air Force is developing the Joint Aerial Layer Network—a system to provide precision timing and navigation signals via aircraft—to substitute temporarily for a loss or degradation of the Global Positioning System (GPS) signal.[54] Another airborne alternative was tested during the 2010 Empire Challenge exercise. A North Atlantic Treaty Organization (NATO) Airborne Warning and Control System (AWACS) aircraft successfully demonstrated the AWACS could operate a Scan Eagle UAV from the air.[55] The ability to use aircraft as a relay or even as a controlling platform lessons reliance on space-based networks.

Aside from bandwidth, cyber defenders and cyber service providers must ensure data is restored. Attackers can either attack the portion of the system that provides the data (the server), the portion of the system that receives the data (the client), the portion of the system that manages the servers, or the data itself. Restoral for the types of attacks that do involve damaging the data is fairly straightforward. It involves restoring the system to a known clean state free of vulnerabilities.

If the data was attacked, the primary difficulty is determining when the data was corrupted and which data is corrupted. Computer forensics provides some of the solution. Forensics is a high-demand, low-availability capability, and the pace of computer

---

Operations, Center for Strategic Leadership Study (Carlisle Barracks, PA: US Army War College, 2006), 53.
[54] Robert K. Ackerman, "Air May Take the Place of Space for Navigation," *Signal Scape*, 4 November 2011, http://www.afcea.org/signal/signalscape/index.php/2011/11/04/14478/ (accessed 22 April 2012).
[55] Dave Majumdar, "Allies Test New Role for AWACS," *C4ISR Journal*, 25 August 2010, http://integrator.hanscom.af.mil/2010/August/08262010/08262010-16.htm (accessed 22 April 2010).

forensics often cannot keep up with dynamic military operations. However, forensic examination determines when and how at attack occurred. If data is manipulated, a reasonable scientific analysis prevents users from unduly losing trust in the system. A Scientific explanation offers causality for an action, which subsequently yields user confidence in future defenses. Forensics, therefore, has strategic significance.

Yet, forensics has not been operationalized, and the technological state of the field would make it hard to do so. The antivirus vendors have some of the field's best technology to analyze malicious code and counter it. However, they took four to five months to undercover all of the details for the Stuxnet worm.[56] This timeframe is not suitable for the battlefield. However, from a resiliency standpoint, the forensic analysis need not be perfect. The analysis requires speed. It should distinguish which data has been corrupted and work in parallel with the system administrator's efforts to restore the system.

To date, cyber forensics in the DOD has been largely associated with law enforcement, gathering evidence, and obtaining convictions. The Defense Computer Forensics Lab and its sister organization, the Defense Cyber Investigations Training Academy, focus on law enforcement and counterintelligence organizations.[57] The area of forensics is underserved and may benefit from research and development attention. In the meantime, the military may be able to outsource some of the forensic analysis in order to leverage the talents of the antivirus vendors and other experts. A timely forensics capability would help allay undue fear and reduce the effectiveness of the enemy's cyber weapons.

Summary

While the ultimate goal is to restore services in a timely manner, there is a tension as to how to accomplish that goal. On one hand, decentralized defenses are more responsive to operational commanders. The operational commanders have direct control over the critical assets that enables their missions. In a decentralized environment, the defenders have a better opportunity to gauge the operational impact of an attack and react

---

[56] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February/March 2011): 27, 36.
[57] Department of Defense Cyber Crimes Center, "About the Academy," http://www.dc3.mil/dcita/dcitaAbout.php (accessed 26 April 2012).

accordingly. On the other hand, the cost of network infrastructure and personnel as well as the need to share common data drives centralization. The cloud computing movement is a good example of this. The primary advantage of cloud computing is reduced cost. In a budget constrained environment, the military should expect costs to predominate much of the decision making process. Thus, the military requires some degree of centralized defense for centralized cyber assets. In reality, not everything in cyberspace is a centralized service. Some level of cyber defense can and currently is pushed to the lowest level. Other networks—such as those that operate the Predator UAV—cannot be feasibly pushed to a regional commander.

Just because a JFC does not have control over all of the portions of cyberspace that enable his mission, it does not absolve him from the responsibility to affect its defense. The JFC should develop a cyber defense element to integrate cyber defense into larger operational and planning elements. Cyber defense should also be integrated with intelligence, counterintelligence, forensics, and network and system administrators. All of the aforementioned functions have mutual dependencies.

Part of the operationalization of cyber defense requires robust situational awareness. As Dr. Kamal Jabbour notes, situational awareness consists of perception, comprehension, and projection. Within the cyber defense paradigm, the defenders must detect the attack, categorize its source and intent, limits harmful effects, apply countermeasures, and restore capability. All of which requires situational awareness and the past, present, and future status of friendly and enemy capabilities. The IPB process for cyberspace helps immensely to achieve the proper perspective to obtain this knowledge.

Aside from situational awareness, the ability to maneuver in cyberspace buys time for cyber defenders relative to the attacker. In one sense, maneuvering to diverse or redundant systems allows defenders to react effectively in a complex system. In another sense, maneuver in cyberspace is weak in relation to other domains. Maneuver in cyberspace does not position one for a kill; rather, its advantage over not maneuvering is the time gained by the defender. In a best case, maneuvering allows defenders to learn more about the enemy, and in doing so, cyber defenders can expose the enemy's attack

methodology. When exposed, cyber defenders can develop countermeasures, and hence, negate the effectiveness of the attacker's weapon.

Situational awareness and maneuverability ultimately lead to negation which leads toward recovery and restoral. Passive cyber defenses will never be perfect, and active defenses will fail if immediacy is the standard. Cyber defenses do not serve to protect the network for the sake of protecting the network. They seek to maintain military power. To be effective, cyber defenses must overcome shortcomings and restore services as soon as possible after an attack. Only then can the military achieve true resiliency.

CHAPTER 6

IMPLICATIONS AND CONCLUSIONS

The military has become reliant on cyberspace. This reliance has been increasing for decades, but Operation Enduring Freedom and Operation Iraqi Freedom drove home how reliant the military is. The military's use of information in war is a vitally important advantage. It allowed a small group of special operations forces to leverage airpower with precision munitions to topple the Taliban government using what amounted to Afghan militia groups. In Iraq, the military defeated the 350,000 person Iraqi Army and overthrew the Saddam Hussein government with inferior numbers of troops in only 28 days of "major combat operations."[1] Though the victory had many factors, the information superiority combat forces enjoyed enhanced their capabilities well beyond their numbers. Information from Blue Force Tracking, aerial surveillance and reconnaissance platforms, intelligence, and logistics units was passed horizontally and vertically throughout the organizational structure. In short, the use of information and cyberspace caused the military to fight differently and more effectively than in past conflicts.

The rest of the world also recognizes these benefits. Senior Colonel Wang Baocun and Li Fei of China's People Liberation Army explain China's move toward more counter-space and network warfare capabilities. They attempt to counter perceived US dominance in cyber technologies.[2] Part of China's anti-access and area-denial strategy incorporates attacks on military cyberspace. In every major scenario of conflict with China (with the exception of Korea), the United States would primarily employ sea and air forces—the forces that are most reliant on information from cyber and space assets.[3] The Chinese use of cyber attacks would degrade the American military's effectiveness

---

[1] Dave Cammons et al., *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume I: Operations*, Center for Strategic Leadership Study (Carlisle Barracks, PA: US Army War College, n.d.), 19-20; Joint Chiefs of Staff, *Operation Iraqi Freedom (OIF) History Brief*, 14 May 2003. Document is now declassified.
[2] Wang Baocun and Li Fei, "Information Warfare," in *Chinese Views of Future Warfare*, ed. Michael Pillsbury (Washington DC: National Defense University Press, 1997), 330-341.
[3] James Dobbins et al., *Conflict with China: Prospects, Consequences, and Strategies for Deterrence*, RAND Occasional Paper (Santa Monica, CA: RAND Corporation, 2011), 5.

and, thus, delay its response. Furthermore, Chinese cyber attacks effectively raise the stakes of the conflict, which may cause American political leaders to recalculate whether military action is desirable.

Cyber attacks have had a significant role in the conflicts between Russia and its former Soviet states. The 2007 cyber attacks on Estonia accompanied what amounted to a diplomatic dispute. In contrast, the 2008 cyber attacks on Georgia came in conjunction with military operations. In both cases, the Russian government had plausible deniability for its involvement in the cyber attacks, although the coordination of military and cyber operations in the Georgian campaign causes the government's denial to be particularly suspect. The message the US military should take from these incidents is that the Russians not only have the capability to launch cyber attacks but the willingness to employ them. The military should also notice that the perpetrators of the attacks may have less than direct involvement with the government. In formulating strategy, the military must include other cyber actors. They must consider not only how to influence a foreign government but also consider a myriad of supporters, surrogates, and sympathizers.

Non-military incidents also shed light on cyber warfare's potential. The Stuxnet worm that degraded uranium production in Iran was not only important because of its effect; it also was clear evidence that determined attacks can impact air-gapped networks. As important as security measures and information assurance are, passive defenses alone will be breached. Moreover, Stuxnet challenged the lingering notion that cyber attacks have to be against internet-connected devices. The Stuxnet incident illustrates why the military must think beyond traditional paradigms on what cyber warfare is and what it can do. Military officers must think creatively to anticipate possible future uses of cyber warfare and to create an environment that fosters resiliency. To help achieve these goals, the military must evaluate and reward officers for their creativity. The culture of both combat units and support units must embrace adaptability. Fundamentally, the military will never become resilient to cyber attacks unless all areas of its organization embrace a "can do" attitude. Creativity and adaptability are cheap. They require no appropriation from Congress; it just has to be natured.

Any discussion of the future of cyber warfare involves relative costs. The monetary costs of finding and exploiting cyber vulnerabilities are relatively low. As discussed in chapter 3, states and non-states can find and develop exploits for common software on the order of tens of thousands of dollars and develop attacks on US infrastructure on the order of hundreds of millions of dollars.[4] The relative low cost of entry changes the distribution of power and potentially gives a variety of groups a power projection capability.

The US military relies on cyberspace to enhance its combat power, but it is also vulnerable to having this capability attacked. The military must prove itself resilient to cyber attacks. How resilient today's military is to cyber attacks is largely unknown. Tactical exercises suggest that the military is somewhat resilient to small-scale attacks. Individual units exercise against enemy jamming and often simulate the loss of a particular capability. The resiliency at the higher levels of war is largely untested.

In general, the prescription of what actions must take place to gain resiliency is fairly straightforward. First, the operating forces must develop alternate procedures in the event of cyber attack against a critical capability and train to these procedures.[5] In other words, the forces must degrade gracefully, a concept that applies to all organizations at all levels of war. No organization can assume they will be immune. Second, cyber defenders must ensure any harmful effects on cyber systems are brief, and they must facilitate the return to normal operating procedures as quickly as possible. Doing so requires a combination of passive defenses, active defense, and ultimately restoral actions. It also requires a degree of diversity. Neither the operating forces nor the cyber defenders can rely on a single system with limited numbers of paths. Rather, they must ensure diversity via the types and numbers of alternative options.

---

[4] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Potomac Books: Dulles, VA, 2009), 183. House. *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security*. 105th Cong., 1st sess., 25 April 2007.

[5] Again, "operating forces" refer to any unit—combat units or support units—that use cyberspace and cyber technologies to accomplish their assigned mission.

Recommendations

Achieving this prescription for resilience requires the military take several measures. The most important measures include accepting opportunity costs, exercise considerations, organizational considerations, and training requirements.

Consider Opportunity Costs

The Commission on Cyber Security for the 44th Presidency concluded that resiliency is the most effective way to deter cyber attacks.[6] The deterrent value and its strategic implications demands resiliency be funded appropriately. Few nations can challenge the United States conventionally. Those that cannot must find seams in the US's security apparatus to exploit. For the US military, the costs of developing and training to alternate procedures that will help close these seams largely boils down to opportunity cost. The operating forces, which are already exceptionally skilled, may lose a few training days on training under normal conditions, but they will gain new insights on how to operate in a degraded environment. The opportunity costs are relatively low.

Exercise Considerations

The military cannot be reactive and expect to be resilient. In chapter 1, the first responders during the Northridge earthquake encountered problems they anticipated and problems they did not. Their resilience allowed them to succeed, but their preparation enabled their resilience. Undoubtedly, the emergency management planners knew they were planning to operate in a complex environment. Even in uncertainty, common trends emerge. In cyber warfare, the enemy can use cyber attacks to cause disruption, deception, or to destroy equipment. When a disruptive attack occurs, commanders should have a heightened state of alert, in case the cyber attack is a prelude to a larger action. The military should also anticipate cyber attacks that intend to cause operators to lose trust in their systems. It also must allow for the possibility that a determined adversary will attempt to use cyberspace a means as an alternative form of global reach, possibly to affect something in the physical environment. From a technical perspective, this requires building a system that anticipates these threats. From a more operational perspective, users must realistically exercise alternate procedures.

---

[6] James R. Langevin et al., *Securing Cyberspace for the 44th Presidency,* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, (Washington, DC: Center for Strategic and International Studies, December 2008), 25-26.

The military presently does not know how resilient it is. Major exercises have specific objectives, take months to plan, and have significant financial costs. Those responsible for the exercise understandably are reluctant to allow cyber red teams to threaten the flow of the exercise. However, by never allowing for the possibility of realistic cyber warfare, the exercise planners miss the big picture. For example, the Air Force only has a few Blue Flag exercises per year to train operators for Air Operations Centers. A major disruption of a planned exercise due to cyber attack would cause operators to lose out on valuable training opportunities. However, even a total loss of one of a Blue Flag exercise would not substantially harm the Air Force's readiness. If cyber attacks would have a major impact on the Air Force's ability to fight and it does not involve realistic cyber attacks against its primary command and control node, the Air Force is only reinforcing a training deficiency. Moreover, the military as a whole must give cyber red teams near free reign during major exercises in order to develop a baseline for its resiliency and to begin the process to develop appropriate tactics and operating procedures at all levels.

Organizational Changes

Exercises, experiments, and practical experience will drive organizational changes to better posture for cyber resiliency. However, some changes are already apparent. For one, the staff structure that gives the communications service provider (the J-6) at combatant commands and joint task forces more stature than the staff officer responsible for integrating cyber warfare is a serious organizational flaw. Cyber defense must be integrated with operational planning, intelligence, counterintelligence, forensics, and information assurance. During mission execution, cyber defenders must coordinate actions they are seeing, gauge the operational impact of the enemy's cyber attacks, and direct appropriate actions. The J-6 is not an appropriate place for these functions, and the J-6's billet and rank could be better employed as a coordinator for cyber warfare. The cyber warfare coordinator should report to the J-3 or directly to the Joint Force Commander (JFC). The JFC should consider transferring the remaining J-6 functions to another staff element. Joint doctrine allows the JFC to place the engineer staff under the J-3, J-4, or as a separate entity depending on the nature of the conflict and how the

engineers will be employed.[7] This model is appropriate for the service provider roles of the J-6 as well. The emphasis needs to shift from providing service to fighting in cyberspace.

Furthermore, the military should accept that many applications and services in military cyberspace will be centralized in a cloud computing architecture, particularly at a time when the military will be looking to reduce support costs. The cost benefits of using clouds will drive the military to this structure. Rather than fighting this trend and insist on control based on traditional military organizational lines, the military should organize its cyber forces around this concept. The difficulty for the organization responsible for defending a cloud is gauging the operational impact in the field.

US Cyber Command's (USCYBERCOM) Cyber Support Element (CSE) must liaise between the JFC, USCYBERCOM, and the cloud defenders. The CSE cannot simply reside with the combatant commander. The dynamic nature of cyber warfare demands that a CSE reside at the lowest level JFC and even at the component level, if necessary. USCYBERCOM must provide oversight of the common services and direct action as necessary. USCYBERCOM also should expand its role beyond the Defense Information Systems Network (DISN) and have the authority to task cyber networks of all kinds that cross combatant command lines of responsibility (e.g., unmanned aerial vehicle command and control networks, defense common ground stations, logistics networks, long-haul communications). If USCYBERCOM is to be the coordinator for military cyberspace, it must have authority for all of military cyberspace not just the DISN portion of it. From the JFC perspective, it needs one organization to solve its external cyber defense needs not several.

These organization changes will place more focus on the role cyberspace plays in operational warfighting. In doing so, the cyber defenders will have more access to and more influence on the operational process. This greater level of understanding should transfer into better planning for cyber attacks, which should yield greater resilience.

Force Development

The tension between quality and cost is readily apparent when considering how to prepare leaders at all levels to operate in the face of cyber attacks. From an operational

---

[7] Joint Publication (JP) 3-34, *Joint Engineer Operations*, 30 June 2011, II-13.

standpoint, junior officers and non-commissioned officers (NCOs) have to be able to operate on their own, since they may face situations where the information to which they have become accustomed is either unavailable or inaccurate. These leaders must have the confidence, judgment, authority, and trust to make decisions in a degraded or denied information environment. Training and experience is required to reach this level of competency. The military must retain these leaders without overtaxing the budget.

In many ways, a smaller force helps this problem, as fewer officers and NCOs will be needed to fulfill these roles. However, the most serious military threat comes from countries that are also some of the world's stronger cyber adversaries. A conflict with these adversaries would require a surge in manpower. Leaders with the experience and competency in a degraded environment cannot be grown in the short term. Military personnel policies must focus on retaining officers and NCOs with both monetary and non-monetary compensation. Part of this package must include incentives to join the reserve component in lieu of complete separation. In an environment that includes cyber warfare, the demands of officership are greater, and the military cannot quickly train new officers if more are needed.

Suggested Additional Research

Since the military only uses a portion of cyberspace, would an increase in the military's resiliency threaten civilian cyber infrastructure? If an adversary develops a cyber attack capability and if it is no longer effective against a more resilient military, would the adversary be content to sit idle? If an adversary cannot achieve its objectives by attacking the military in cyberspace, does it turn its cyber force against civilian systems? During World War II, the United Kingdom's Royal Air Force and the US Army Air Corps justified targeting German and Japanese cities as a way to end the war and because they were unable to achieve the desired effect on military targets.[8] The Germans' use of unrestricted submarine warfare is another case where civilian assets were targeted in lieu of the more powerful British Navy.

If an adversary has a capability to attack either military or civilian cyberspace, why would it not attack both? The rational decision would be to attack the target that

[8] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare*, 3rd ed. (Princeton, NJ: Princeton University Press, 2004), 184-203, 261-270.

yields the most value to obtain a political objective. Resources may constrain a cyber force from being able to attack every valuable target. If the military becomes more resilient to cyber attacks, the enemy may focus his efforts elsewhere.

Another area of potential additional research is how the concept of consequence management applies in cyberspace. Regardless if the military portion or the civilian portion of cyberspace is the target, there is a strong likelihood of spillover effects from cyber attacks. The military has both the need to protect the nation from external attack and a reliance on civilian infrastructure. The notion of resiliency within the military is important for its own operations. Eventually, the lessons the military will learn must be shared with and integrated into the other segments of American government and, indeed, the American society to preserve national security.

Resilience will remain an important aspect of American cyber warfare strategy. A fortress mentality will not work and security costs will to escalate. Security measures can never be 100 percent. The United States military has built a force structure that relies on information. It must not allow cyberspace to become its Achilles' heel.

ACRONYMS

AOC – Air Operations Center

AWACS – Airborne Warning and Control System

BFT – Blue Force Tracking

C2 – Command and Control

CAC – Common Access Card

CAD – Computer-Aided Design

CAOC – Combined Air Operations Center

CD-ROM – Compact Disc—Read-Only Memory

COCOM – Combatant Commander

CSE – Cyber Support Element

DAA – Designated Approval Authority

DISA – Defense Information Systems Agency

DOD – Department of Defense

DISN – Defense Information Systems Network

DSN – Defense Switched Network

FBCB2 – Force XXI Battle Command Brigade and Below

GDP – Gross Domestic Product

GPS – Global Positioning System

IP – Internet Protocol

IPB – Intelligence Preparation of the Battlefield

ISR – Intelligence, Surveillance, and Reconnaissance

JDAM – Joint Direct Attack Munition

JFC – Joint Force Commander

JWICS – Joint Worldwide Intelligence Communications System

MIT – Massachusetts Institution of Technology

NASA – National Aeronautics and Space Administration

NATO – North Atlantic Treaty Organization

NCO – Non-Commissioned Officer

NIPRNET – Non-Secure Internet Protocol Routed Network

OEF – Operation Enduring Freedom

OIF – Operation Iraqi Freedom

ROE – Rules of Engagement

SCADA – Supervisory Control and Data Acquisition

SIPRNET –Secure Internet Protocol Routed Network

SOF – Special Operations Forces

TCP/IP – Transmission Control Protocol/Internet Protocol

UAV – Unmanned Aerial Vehicle

UN – United Nations

USCENTCOM – United States Central Command

USCYBERCOM – United States Cyber Command

BIBLIOGRAPHY

309 Software Maintenance Group. “Mission Planning.” http://www.309smxg.hill.af.mil/solutions/mission_planning.html (accessed 1 May 2012).

Ackerman, Robert K. “Air Force Communicators Move Faster, Lighter.” *Signal*, September 2002, 47.

Ackerman, Robert K. “Air May Take the Place of Space for Navigation.” *Signal Scape*, 4 November 2011. http://www.afcea.org/signal/signalscape/index.php/2011/11/04/14478/ (accessed 22 April 2012).

Ackerman, Robert K. “Operation Enduring Freedom Redefines Warfare.” *Signal*, September 2002, 3-5.

Ackerman, Robert K. “Special Operations Forces Become Network-Centric.” *Signal*, March 2003, 17.

Allen, Patrick D. *Information Operations Planning*. Norwood, MA: Artech House, 2007.

Authorization of the Use of Military Force Against Iraq of 2002. Public Law 107-243. 107th Cong., 2nd sess., 16 October 2002.

Anderson, Levon R. “Countering State-Sponsored Cyber Attacks: Who Should Lead?” Research paper, US Army War College, March 2007.

Andress, Jason, and Steve Winterfield. *Cyber Warfare: Techniques, Tactics, and Tools for Cyber Practitioners*. Waltham, MA: Syngress, 2011.

Baocun, Wang, and Li Fei. “Information Warfare.” In *Chinese Views of Future Warfare*, edited by Michael Pillsbury, 327-342. Washington DC: National Defense University Press, 1997.

Baumgardner, Neil. “3rd Infantry Division Commander Praises C2V, Communications during OIF.” *Defense Daily* 218, no. 34 (16 May 2003): 1.

BBC News. “Estonia Fines Man for ‘Cyber War.’” 25 January 2008. http://news.bbc.co.uk/2/hi/technology/7208511.stm.

Beeker, Kevin R. “Strategic Deterrence in Cyberspace.” Master’s thesis, Air Force Institute of Technology, June 2009.

Berlocher, Greg. “Military Continues to Influence Commercial Operators.” *Satellite Today*, 1 September 2008. http://www.satellitetoday.com/military/netwarfare/Military-Continues-To-Influence-Commercial-Operators_24295_p2.html (accessed 15 January 2012).

Beyerchen, Alan. “Clausewitz, Nonlinearity, and the Unpredictability of War.” *International Security* 17, no. 3 (Winter 1992-1993): 59-90.

Biddle, Stephen. “Afghanistan and the Future of Warfare.” *Foreign Affairs* 82, no. 2 (March/April 2003): 31-46.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare*, 3rd ed. Princeton, NJ: Princeton University Press, 2004.

Bitar, Imad, and Brian L. Felsman. “Blue Force Tracking in Operation Enduring and Iraqi Freedom.” *Technology Review Journal* 13, no. 2 (Fall/Winter 2005): 79-97.

Boland, Rita. “When Capabilities and Support Mean Life or Death.” *SIGNAL Magazine*, March 2011.

http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2550&zoneid=285 (accessed 18 January 2012).

Boyle, Rebecca. "Proof-of-Concept CarShark Software Hacks Car Computers, Shutting Down Brakes, Engines, and More." *Popsci.com*, 14 May 2010. http://www.popsci.com/cars/article/2010-05/researchers-hack-car-computers-shutting-down-brakes-engine-and-more (accessed 4 April 2012).

Briefing. MITRE Corporation. Subject: Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia, August 2008.

Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, 15 January 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all.

Briscoe, Bob, Andrew Odlyzko, and Benjamin Tilly. "Metcalfe's Law is Wrong." *IEEE Spectrum*, July 2006. http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong (accessed 26 January 2012).

Bureau of Economic Analysis. "National Income and Product Accounts: Gross Domestic Product, 4th Quarter and Annual 2011 (Advance Estimate)." 27 January 2012. http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm.

Bureau of the Public Debt. "Monthly Statement of the Public Debt of the United States." 31 January 2012. http://www.treasurydirect.gov/govt/reports/pd/mspd/2012/opds012012.pdf (accessed 31 January 2012).

Burgoon, Judee K., and Jay F. Nunamaker, Jr., eds., "Toward Computer-Aided Support for the Detection of Deception." *Group Decision and Negotiation* 13 (2004): 1-4.

Bush, George W. "Address Before a Joint Session of Congress on the United States Response to the Terrorist Attacks of September 11." Compilation of Presidential Documents, 37 WCPD 1347 (20 September 2001): 1347-1351. http://www.gpo.gov/fdsys/pkg/WCPD-2001-09-24/pdf/WCPD-2001-09-24-Pg1347.pdf (accessed 28 April 2012).

Bush, George W. "Address to the Nation on Iraq." Compilation of Presidential Documents, 39 WCPD 338 (17 March 2003): 338-341. http://www.gpo.gov/fdsys/pkg/WCPD-2003-03-24/pdf/WCPD-2003-03-24-Pg338-2.pdf (accessed 28 April 2012).

Bush, George W. "Address to the United Nations General Assembly in New York City." Compilation of Presidential Documents, 38 WCPD 1529 (11 September 2002): 1529-1533. http://www.gpo.gov/fdsys/pkg/WCPD-2002-09-16/pdf/WCPD-2002-09-16-Pg1529.pdf (accessed 28 April 2012).

Caesar, Ed. "Bradley Manning: Wikileaker." *The Sunday Times*, 19 December 2010. http://www.edcaesar.co.uk/article.php?article_id=53 (accessed 30 April 2012).

Cammons, Dave, John B. Tisserand, III, Duane E. Williams, Alan Seise, and Doug Lindsay. *Network-centric Warfare Case Study: US V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume I: Operations*. Carlisle Barracks, PA: US Army War College, 2006.

Caudle, Daryl L. "Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers." PhD diss., University of Phoenix, Oct 2010.

Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership*, 8 February 2011.

Chilton, Kevin P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities." *Air and Space Power Journal* 23, no. 3 (Fall 2009). http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/chilton.html (accessed 15 April 2012).

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Clowney, Patrick. "Clausewitz and Network Centric Warfare: A Beautiful Message." *High Frontier* 5, no. 3 (May 2009): 38-41.

Cogen, Kevin J., and Raymond G. DeLucio, *Network-centric Warfare Case Study: US V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Arp 2003)*, *Volume II*, *A View of Command, Control, Communications, and Computer Networks at the Dawn of Network-centric Warfare*. Carlisle Barracks, PA: US Army War College, 2006.

Cohen, Fred. "A Note on the Role of Deception in Information Protection." Fred Cohen and Associates, 1998. http://all.net/journal/deception/deception.html (accessed on 7 April 2012).

Collier, Mike. "Estonia: Cyber Superpower." *Business Week*, 17 Dec 2007. http://www.businessweek.com/globalbiz/content/dec2007/gb20071217_535635.htm (accessed 16 March 2012).

Comfort, Louise K. "Risk and Resilience: Interagency Learning Following the Northridge Earthquake of 17 January 1994," *Journal of Contingencies and Crisis Management* 2, no. 3 (September 1994): 157-170.

Congressional Budget Office. "Budget Projections." Table 1-1. http://www.cbo.gov/ftpdocs/126xx/doc12699/BudgetProjections.xls.

Crowell, Richard M. "War in the Information Age: A Primer for Cyberspace Operations in the 21st Century." Newport, RI: Naval War College, 2010.

"Cyberwar." *Economist* 396, no. 8689 (3 July 2010): 11-12.

Department of Commerce. *The NIST Definition of Cloud Computing*. Special Publication 800-145. Washington, DC: National Institute of Standards and Technology, September 2011.

Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.

Department of Defense. *The Implementation of Network-Centric Warfare*. Washington DC: Office of Force Transformation, n.d.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Office of the Secretary of Defense, July 2011.

Department of Defense. *Report of the Defense Science Board on Enhancing Adaptability of US Military Forces: Part A, Main Report*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2011.

Department of Defense. *Sustaining US Global Leadership: Priorities for 21st Century Defense*. Washington, DC: Office of the Secretary of Defense, January 2012.
Department of Defense Cyber Crimes Center. "About the Academy." http://www.dc3.mil/dcita/dcitaAbout.php (accessed 26 April 2012).
Department of Defense Directive (DODD) 3020.40. *DOD Policy and Responsibilities for Critical Infrastructure*, 14 January 2010, incorporating Change 1, 1 July 2010.
Department of Defense Directive (DODD) 8500.01E. *Information Assurance (IA)*, 24 October 2002.
Department of the Air Force. *Report on Defending and Operating in a Contested Cyber Domain*. SAB-TR-08-01. Washington, DC: United States Air Force Scientific Advisory Board, 31 August 2008.
Department of the Air Force. *Report on Implications of Cyber Warfare, Volume 2: Final Report*. SAB-TR-07-02. Washington DC: United States Air Force, August 2007.
Department of the Army. *Critical Infrastructure Threats and Terrorism.* DCSINT Handbook no. 1.02. Ft Leavenworth, KS: Training and Doctrine Command, 15 August 2005.
Dizzard, Wilson P., III., "Spy Agencies Adapt Social Software, Federated Search Tools." *Government Computer News*, 22 September 2006. http://gcn.com/articles/2006/09/22/spy-agencies-adapt-social-software-federated-search-tools.aspx.
Dobbins, James, David C. Gompert, David A. Shlapak, and Andrew Scobell. *Conflict with China: Prospects, Consequences, and Strategies for Deterrence*. RAND Occasional Paper. Santa Monica, CA: RAND Corporation, 2011.
Dumiak, Michael. "Casus Belli." *Defense Technology International* 4, no. 8 (1 September 2010): 31.
Edwards, John. "Commercial Sat Market Stirs." *Aviation Week and Space Technology* 162, no. 3 (17 January 2005): 147-150.
Eovito, Brian A. "The Impact of Synchronous Text-Based Chat on Military Command and Control." Paper presented at the 11th Information Command and Control Technology Symposia, Cambridge, UK, September 2006.
Falliere, Nicholas, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier," version 1.4 (February 2011). Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
Fallows, James. "Cyber Warriors." *The Atlantic*, March 2010, 58-63.
Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival: Global Politics and Strategy* 53, no. 1 (February/March 2011): 23-40.
Federal Trade Commission. "FTC Releases Survey of Identity Theft in the US Study Shows 8.3 Million Victims in 2005." http://www.ftc.gov/opa/2007/11/idtheft.shtm (accessed 15 March 2012).
Field Manual (FM) 34-130. *Intelligence Preparation of the* Battlefield, 8 July 1994.
Finley, Bruce. "Intelligence Fixes Floated at Conference." *Denver Post*, 22 August 2006. http://www.denverpost.com/search/ci_4216851.
Fischer, David, and Dennis B. Smith. "Emergent Issues in Interoperability." *News at SEI*, 1 March 2004. http://www.sei.cmu.edu/library/abstracts/news-at-sei/eyeonintegration20043.cfm (accessed 12 March 2012).

Fryer-Biggs, Zachary. “US Military Goes on the Cyber Offensive.” *Federal Times*, 26 March 2012. http://www.federaltimes.com/article/20120326/DEPARTMENTS01/203260301/ (accessed 21 April 2012).

Fulghum, David A., and Robert Wall. “US Electronic Surveillance Monitored Israeli Attack on Syria.” *Aviation Week*, 21 November 2007. http://www.aviationweek.com/aw/generic/story.jsp?id=news/ISRA112107.xml&headline=U.S.%20Electronic%20Surveillance%20Monitored%20Israeli%20Attack%20On%20Syria&channel=defense (accessed 21 February 2012).

Gallagher, Sean. “Satcom at a Crossroads.” http://defensesystems.com/articles/2009/06/10/tech-focus-satellite-communications.aspx (accessed 15 January 2012).

Garstka, John J. “Network-Centric Warfare Offers Warfighting Advantage.” *Signal*, May 2003, 58.

Gates, Robert M. Secretary of Defense. To Secretaries of Military Departments; Chairman of the Joint Chiefs of Staff; Deputy Chief Management Officer; Commanders of the Combatant Commands; Assistant Secretaries of Defense; General Counsel of the Department of Defense; Director, Operational Test and Evaluation; Director, Cost Assessment and Program Evaluation; Inspector General of the Department of Defense; Assistants to the Secretary of Defense; Director, Administration and Management; Director, Net Assessment; Directors of the Defense Agencies; Directors of the DOD Field Activities. Memorandum, 23 June 2009.

Gloystein, John W. “Cyberdeterrence in 2035.” Research paper, Air War College, February 2010.

Gonzales, Daniel, John Hollywood, Gina Kinston, and David Signori. *Network-centric Operations Case Study: Air-to-Air Combat with and without Link-16*. Santa Monica, CA: RAND Corporation, 2005.

Gonzales, David, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, and Michael Tseng. *Network-Centric Operations Case Study: The Stryker Brigade Combat Team*. Santa Monica, CA: Rand Corporation, 2005.

Google. “Technology Overview.” http://www.google.com/about/corporate/company/tech.html (accessed 23 January 2012).

Government Accountability Office. *Critical Infrastructure Protection: Challenges and Efforts to Control Systems*. GAO-04-354. Washington, DC: Government Accountability Office, March 2004,

Gray, Colin S. *Explorations in Strategy*. Westport, CT: Praeger, 1998.

Groh, Jeffrey L. “Network-centric Warfare: Leveraging the Power of Information.” In *US Army War College Guide to National Security Issues, Vol. 1: Theory of War and Strategy*, 3rd ed. Carlisle Barracks, PA: Army War College, 2008.

Hansen, Andrews P. “Cyber Flag: A Realistic Cyberspace Training Construct.” Masters’ thesis, Air Force Institute of Technology, March 2008.

Hare, Forest B., and Glenn Zimmerman. “The Air Force in Cyberspace: Five Myths of Cyberspace Superiority.” In *Military Perspectives on Cyberspace*, edited by Larry

K. Wentz, Charles L. Barry, and Stuart H. Starr. Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009.

Hernandez, Johnnie. "The Human Element Complicates Cybersecurity." *Defense* Systems, 2 March 2010. http://defensesystems.com/Articles/2010/03/11/Industry-Perspective-1-human-side-of-cybersecurity.aspx?Page=2 (accessed 21 March 2012.

Hodge, Nathan, Julian E. Barnes, and Adam Entous. "Pentagon Unveils Spending Plan for Fiscal 2013." *Wall Street Journal Online*, 26 January 2012. http://online.wsj.com/article/BT-CO-20120126-714664.html (accessed 26 January 2012).

Hoffman, F.G. *Homeland Security: A Comparative Strategies Approach*. Washington, DC: Center for Defense Information, March 2002.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, 2.

Hoover, J. Nicholas. "Former Intelligence Chief: US Would Lose Cyberwar." *Information Week*, 23 February 2010. http://www.informationweek.com/news/government/security/223100425 (accessed 23 January 2012).

HQ AF/XOL. "Operation Anaconda: An Air Power Perspective." Staff study, 7 February 2005.

Jabbour, Kamal. "The Science and Technology of Cyber Operations." *High Frontier* 5, no. 3 (May 2009): 11-15.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010.

Joint Publication (JP) 3-13. *Information Operations*, 13 February 2006.

Joint Publication (JP) 3-33. *Joint Task Force Headquarters*, 16 February 2007.

Joint Publication (JP) 3-34. *Joint Engineer Operations*, 30 June 2011.

Johnson, David E., and Steve Pettit. "Principles of the Defense for Cyber Networks: An Executive Overview." *Defense Concepts* 4, no. 4 (Winter 2010): 15-21.

Kaufman, Alfred. "Caught in the Network: How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy." *Armed Forces Journal*, 1 February 2005, 20-22.

Kelly, C. "Guidelines for Trust in Future ATM Systems: A Literature Review." European Air Traffic Management Programme Technical Document. Brussels: European Organisation for the Safety of Air Navigation, 2003.

Kick, Jason. "Cyber Warfare Exercise Overview." MITRE Report, MTR 05B0000052, August 2005.

Kennett, Lee. *The Air War: 1914-1918*. New York: Free Press, 1999.

Knight, Scott, and Sylvain LeBlanc. "When Not to Pull the Plug: The Need for Counter-Surveillance." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers. Fairfax, VA: IOS Press, 2009.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-42. Dulles, VA: Potomac Books, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin P. Kramer, Stuart H. Starr, and Larry K. Wentz. Dulles, VA: Penguin Books, 2009.

Kundra, Vivek. *Federal Cloud Computing Strategy*. Washington, DC: US Chief Information Officer, 8 February 2011.

Langevin, James R., Michael T. McCaul, Scott Charney, and Harry Raduege. *Securing Cyberspace for the 44th Presidency.* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC: Center for Strategic and International Studies, December 2008.

Leder, Felix, Tillman Werner, and Peter Martini. "Proactive Botnet Countermeasures: An Offensive Approach." in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers. Fairfax, VA: IOS Press, 2009.

Lewis, James A. "Thresholds for Cyberwar." Center for Strategic Studies Report. Washington, DC: Center for Strategic Studies, September 2010.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future* London: Frank Cass, 2004.

Lukasik, Stephen J., Seymour E. Goodman, and David W. Longhurst. *Protecting Critical Infrastructure against Cyber Attacks.* New York, Oxford University Press, 2003.

Lynn, William J., III. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.

Madhaven, P., and D. A. Wiegmann. "Similarities and Difference between Human-Human and Human-Automation Trust: An Integrative Review." *Theoretical Issues in Ergonomics Study* 8, no. 4 (July-August 2007): 277-301..

McCarthy, John A. "From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum." In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, 1-7. Arlington, VA: George Mason School of Law, February 2007.

Meserve, Jeanne. "Mouse Click Could Plunge a City into Darkness, Experts Say." *CNN.com*, 27 September 2007. http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US.

Moffat, James. *Complexity Theory and Network Centric Warfare*. Washington, DC: CCRP, 2003.

Moffat, James. "Modeling Human Decision-Making." *The International C2 Journal* 1, no. 1 (2007): 31-60.

Majumdar, Dave. "Allies Test New Role for AWACS." *C4ISR Journal*, 25 August 2010. http://integrator.hanscom.af.mil/2010/August/08262010/08262010-16.htm (accessed 22 April 2010).

Ogielski, Andy. "Securing the Global Network Infrastructure." White paper, Renesys Corporation, 2005. http://www.renesys.com/tech/notes/WP_SGNI_rev2.pdf (accessed 18 January 2012).

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics regarding US Acquisition of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.

Page, Scott E. *Diversity and Complexity*. Princeton, NJ: Princeton University Press, 2011.

Parasuraman, Raja, Robert Molloy, and Indramani L. Singh. "Performance Consequences of Automation-Induced 'Complacency.'" *The International Journal of Aviation Psychology* 3, no. 1 (January 1993): 1-23.

Peltz, Eric, John M. Halliday, Marc L. Robbins, and Kenneth J. Girardini. *Sustainment of Army Forces in Operation Iraqi Freedom: Battlefield Logistics and Effects on Operations*. Santa Monica, CA: RAND Corporation, 2005.

Pringle, Rodney. "NCW Changing Urban Warfare, Official Says." *Aviation Week*, n.d. http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?headLine=NCW%20Changing%20Urban%20Warfare,%20Official%20Says%20%20&storyID=news/NCW02035.xml (accessed 21 February 2012).

Pommerening, Christine. "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm." In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, 9-21. Arlington, VA: George Mason School of Law, February 2007.

Ratcliff, R. A. *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. Cambridge, UK: Cambridge University Press, 2006.

Rattray, Gregory J. "An Environmental Approach to Cyberpower." In *Cyberpower and Cyberdeterrence*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books: Dulles, VA, 2009.

Repik, Keith. "Defeating Adversary Network Intelligence Effort with Active Cyber Defense Techniques." Master's thesis, Air Force Institute of Technology, June 2008.

Report of CENTAF Assessment and Analysis Division. "Operation Iraqi Freedom – By the Numbers." 30 April 2003. http://www.globalsecurity.org/military/library/report/2003/uscentaf_oif_report_30apr2003.pdf (accessed 22 February 2012).

Rios, Billy K. "Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack." in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers. Amsterdam: Ios Press, 2009.

Rosenzweig, Paul. "National Security Issues in Cyberspace." Post workshop report of the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum, Annapolis, MD, September 2009.

Rothschild, Jeff. "High Performance at Massive Scale – Lessons Learned at Facebook." Address. University of California, San Diego, 8 October 2009.

Schmitt, Eric, and Thom Shanker. *Counterstrike: The Untold Story of America's Secret War Against Al Qaeda*. New York: Times Books, 2011.

Schmitt, Michael N. "The Sixteenth Waldemar A. Solf Lecture in International Law." *Military Law Review* 176: 364-421.

Schoorman, F. David, Roger C. Mayer, and James H. Davis. "An Integrative Model of Organizational Trust: Past, Present, and Future." *Academy of Management* Review 32, no. 2 (April 2007): 344-354.

Schrage, Michael. "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency." Security Studies Working Paper E38-600. Cambridge, MA: Massachusetts Institute of Technology, May 2003.

Skoudis, Edward. "Information Security Issues in Cyberspace." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books: Dulles, VA, 2009.

Sirak, Michael, and Marc Schanz. "Air Force World." *Air Force Magazine* 91, no. 7 (July 2008): 12-20.

Slabodkin, Greg. "DISA Outlines Major Network and Enterprise Initiatives." *Defense Systems*, 1 April 2011. http://defensesystems.com/Articles/2011/03/29/Cover-Story-DISA-charts-cloud-strategy.aspx (accessed 7 April 2012).

Smith, Jeffrey H. "Symposium: State Intelligence Gathering and International Law: Keynote Address," *Michigan Journal of International Law* 28 (Spring 2007): 543-552.

Starr, Stuart H. "Toward a Preliminary Theory of Cyberspace." In *Cyberpower and Cyberdeterrence*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books: Dulles, VA, 2009.

Starr, Stuart H. "Towards and Evolving Theory of Cyberspace." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 43-88. Fairfax, VA: IOS Press, 2009.

Strang, Adam J., Benjamin A. Knott, Gregory J. Funke, Sheldon M. Russell, Brent T. Miller, Allen W. Dukes, April M. Courtice, Joseph Lyons, Rebecca D. Brown, James Hyson, and Robert S. Bolia. "Collaboration Technologies Improve Performance and Communication in Air Battle Management." *Military Psychology* 23, no 4. (2011): 390-409.

Sternstein, Aliya. "Defense Cyber Chief: The Cloud is the Military's Next Internet." *Nextgov.com*, 27 October 2011. http://www.nextgov.com/cloud-computing/2011/10/defense-cyber-chief-the-cloud-is-the-militarys-next-internet/50023/ (accessed 30 April 2012).

Stewart, Richard W. *Operation Enduring Freedom: The United States Army in Afghanistan, October 2001-March 2002*. Washington, DC: Center for Military History, 2004.

Stiennon, Richard. *Surviving Cyber War*. Lanham, MD: Government Institutes, 2010.

Sun Tzu, *The Illustrated Art of War*, translated by Samuel B. Griffith. Oxford: Oxford University Press, 2005.

Kheng Lee Gregory Tan. "Confronting Cyberterrorism with Cyber Deception." Master's thesis, Naval Postgraduate School, December 2003.

Tisserand, John B., III. *Network-centric Warfare Case Study: US V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003), Volume III: Network-centric Warfare Insights*. Carlisle Barracks, PA: Center for Strategic Leadership, 2006.

U.K. House of Commons Library. *Cyber Security: A New National Programme*, by Emma Downing. Standard Note SN/SC/5832. London: Parliament, 23 June 2001.

United States Africa Command. "Operation Enduring Freedom Trans Sahara." http://www.africom.mil/oef-ts.asp (accessed 21 February 2012).

United States Air Force. "Blue Flag." 3 March 2010. http://www.505ccw.acc.af.mil/library/factsheets/factsheet.asp?id=15317 (accessed 21 March 2012).

United States Air Force. "Predator Combat Air Patrols Double in 1 Year." 6 May 2008. http://www.af.mil/news/story.asp?id=123097395 (accessed 23 January 2012).

US Cyber Command Public Affairs. "US Cyber Command." US Strategic Command, December 2011. http://www.stratcom.mil/factsheets/cyber_command/ (accessed 14 March 2012).

US House. *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security*. 105th Cong., 1st sess., 25 April 2007.

US House, *Cyber-Terrorism: Hearing before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services*. 108th Cong., 1st sess., 24 July 2003. Statement by Major General James D. Bryan, www.dod.mil/dodgc/olc/docs/test03-07-24Bryan.doc.

US Library of Congress, Congressional Research Service. *Network-centric Operations: Background and Oversight Issues for Congress*, by Clay Wilson, CRS Report RL32411. Washington, DC: Office of Congressional Information and Publishing, 15 March 2007.

Van Creveld, Martin. *Command in War*. Cambridge, MA: Harvard University Press, 1985.

Virden, Roy John. "Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems." Research Paper, Naval War College, 3 February 2003.

Wass de Czege, Huba. "Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack." *Military Review*, July-August 2010.

Waters, Gary. "The Australian Defence Force and Network-centric Warfare." In *Australia and Cyber Warfare*, edited by Gary Waters, Desmond Ball, and Ian Dudgen. Canberra: ANU E Press, 2008.

Weinstein, John M. "Ten Reasons Why Nuclear Deterrence Could Fail: The Case for Reassessing US Nuclear Policies and Plans." In *Deterrence for the 21st Century*, edited by Max G. Manwaring. Portland, OR: Frank Cass, 2001.

Werner, Debra. "Satellite Security: Hacking Cases Draw Attention to Satcom Vulnerabilities." *C4ISR Journal* 11, no. 1 (January/February 2012): 16-18.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011.

The White House. *National Security Strategy*, May 2010.

Wiegmann, Douglas A., Aaron Rich, and Hui Zhang. "Automated Diagnostic Aids: The Effects of Aid Reliability on Users' Trust and Reliance." *Theoretical Issues in Ergonomic Science* 2, no. 4 (2001): 352-367.

Wilson, Clay. "Cyber Crime." In *Cyberpower and Cyberdeterrence*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books: Dulles, VA, 2009.

Wingfield, Thomas C. "International Law and Information Operations." In *Cyberpower and Cyberdeterrence*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books: Dulles, VA, 2009.

Winterfield, Steven P. "Cyber IPB." GSEC paper submission, December 2001. http://www.giac.org/paper/gsec/1752/cyber-ipb/103147 (accessed 15 April 2012).

Yuill, Jim, Dorothy Denning, and Fred Feer. "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques." *Journal of Information Warfare* 5, no 3. (November 2006): 26-40.